BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR THE INTERNET OF THINGS AND HOME NETWORKS

by

Diego M. Mendez Mena

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Department of Computer and Information Technology

West Lafayette, Indiana

May 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL

STATEMENT OF COMMITTEE APPROVAL

Dr. Baijian Yang, Chair

Department of Computer and Information Technology

Dr. J. Eric Dietz

Department of Computer and Information Technology

Dr. Wenhai Sun

Department of Computer and Information Technology

Dr. Victor Raskin

Department of English

Approved by:

Dr. Kathryne A. Newton

Associate Dean for Graduate Programs

To my daughter Lana, you are my inspiration, I love you.

To my loving wife Mayari, this wouldn’t have been possible without you.

To my parents, Miguel and Cecilia, and my sister Carolina. My compass and support.

ACKNOWLEDGMENTS

I would like to express my gratitude to my advisor, Prof. Baijian Yang. I value the mentoring, insights, and guidance you have provided. Also, I would like to extend this feeling to the Purdue Polytechnic Institute, the Computer and Information Technology Department, the Purdue Center for Education and Research in Information Assurance and Security (CERIAS), as well as my Graduation Committee. And most importantly, to my family for their support and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIS	Artificial Immune System
ABA	Anomaly Based Analysis
AH	Authentication Header
AA	Automated Agents
BTC	Bitcoin
BFT	Byzantine Fault Tolerance
CA	Certificate Authority
C&C	Command-and-Control
CoAP	Constrained Application Protocol
CIDR	Classless Inter-Domain Routing
CPE	Costumer Premises Equipment
CybOX	Cyber Observable Expression
CTI	Cyber Threat Information
CPU	Central Processing Unit
dAPP	Decentralized application
DAO	Decentralized Autonomous Organizations
DHS	Department of Homeland Security
DoS	Denial-of-Service
DDoS	Distributed-Denial-of-Service
ECC	Elliptic Curve Cryptography
ESP	Encapsulating Security Payload
EVM	Ethereum Virtual Machine
GK	Gatekeeper
GRE	General Routing Encapsulation
GB	Gigabytes
GNS3	Graphical Network Simulator-3
HTTP	HyperText Transfer Protocol
IACAC	Identity Authenticaiton and Capability based Access Control

ICMP	Internet Control Message Protocol
IP	Internet Protocol
IDS	Intrusion Detection System
IOC	Indicators of Compromise
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPFS	InterPlanetary File System
ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
LoWPAN	Low-Power Wireless Personal Area Networks
LA	Learning Automata
OASIS	Organization for Advancement of Structured Information Standards
ONOS	Open Network Operating System
PDF	Portable Document Format
P2P	Peer-to-Peer
PSK	Pre-Shared Key
PSI	Private Set Intersection
PoA	Proof of Authority
PoC	Proof-of-Concept
PoS	Proof-of-Stake
PHI	Protected Health Information
PoW	Proof of Work
PKI	Public Key Infrastructure
RAM	Random Access Memory
RSA	Rivest–Shamir–Adleman public-key cryptosystem
MITM	Man-in-the-Middle
MB	Megabyte
NRT	Near Real Time
SHA	Secure Hash Algorithm
SP	Service Provider(s)

SDN	Software Defined Networking
SDX	Software Defined Everything
STIX	Structured Threat Information eXpression
SHM	Symmetric Homomorphic Mapping
SYN	Synchronize Transfer Control Protocol Packet
Tbps	Terabytes Per Second
TCBI	Threshold Credit-Based Incentives
TTM	Time to Market
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TCP	Transfer Control Protocol
TAXII	Trusted Automated Exchange of Indicator Information
URL	Uniform Resource Locator
WSN	Wireless Sensor Networks
ZB	Zettabytes

GLOSSARY

Bitcoin – First open-to-public cryptocurrency that is able to complete peer-to-peer financial transactions without a centralized entity that uses the blockhain as the underlying technology.

Blockchain – Crytographically-based data blocks that are unidirectionally linked to others tocreate a immutable and decentralized record of growing electronic transactions, a distributed ledger.

Cryptocurrency – Electronic-based medium of exchange that utilizes the blockchain to keep a distributed and immutable ledger of all transactions.

Ethereum – An open-source cryptocurrency platform that includes, besides basic cryptocurrency features, Touring-complete computing capabilities that reside on their own version of the blockchain technology.

Internet of Things – "Envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable... The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration". (Minerva, Biru, & Rotondi, 2015, p. 74)

Proof of Work – Protocol used by some blockchain platforms, including Bitcoin and Ethereum,that verifies transactions to prevent double-spending by using computing power to calculate hash values embedded into transaction blocks.

ABSTRACT

During recent years, attacks on Internet of Things (IoT) devices have grown significantly. Cyber criminals have been using compromised IoT machines to attack others, which include critical internet infrastructure systems. Latest attacks increase the urgency for the information security research community to develop new strategies and tools to safeguard vulnerable devices at any level. Millions of intelligent things are now part of home-based networks that are usually disregarded by solutions platforms, but not by malicious entities. Therefore, the following document presents a comprehensive framework that aims to secure home-based networks, but also corporate and service provider ones. The proposed solution utilizes first-hand information from different actors from different levels to create a decentralized privacy-aware Cyber Threat Information (CTI) sharing network, capable of automate network responses by relying on the secure properties of the blockchain powered by the Ethereum algorithms.

CHAPTER 1. INTRODUCTION

In this chapter, the author established an outline of the current research document. The author reviewed the technological conjuncture, provided the scope, shows the significance, and laid out the research questions determined by assumptions and limitations. Finally, the author concludes with an overview of this work.

1.1 Background

The Internet of Things (IoT) is comprised of resource-constrained devices connected to the internet and interacting with other networks with or without direct human intervention. The IoT's primary objective is to maintain operations regardless of location to provide seamless interaction between users and "things" to transfer and/or retrieve data, and respond with intelligent actions (Mendez Mena, Papapanagiotou, & Yang, 2018). The last few years, the performance and capabilities of IoT devices have improved, nevertheless, the security of IoT devices has not kept the pace and it remains as the main challenge to address. In October 2016, the major internet service provider Dyn suffered a major Denial-of-Service (DoS) attack by an army of compromised IoT machines, which has increased the urgency to deal with ill-protected IoT devices (Krebs, 2016). Forbes (2016) believed that by 2020, the Internet of Things would exchange over 40 Zettabytes of data (Forbes, 2016) as over 20 billion devices interact over the internet (Gartner, 2017), increasing the risk spectrum significantly for the IoT.

A main property for IoT devices is to be ubiquitous, which entails requirements for power efficiency as well as limited computing capabilities that do not drain the power of the device. Such intrinsic properties are found to contradict cryptography-based applications and other securing algorithms, making the IoT security environment even more challenging (Mendez Mena et al., 2018). Nevertheless, security researchers have paid attention to new technologies that could help to cope with the current computing, energy, and security necessities of the IoT. The blockchain and its cryptocurrency applications have disrupted the Internet environment over the last few years, providing a new way to securely transact digital assets by combining reliable cryptographic principles and secure protocols. The IoT security community has been trying to use the blockchain's strengths to make embedded devices less prone to cyberattacks.

The purpose of this work was to present an application of the blockchain protocol to protect networks at different levels and, therefore, the IoT devices in it. Also, this document introduced a security framework that uses the blockchain to share security intelligence, gathered directly from cyber targets, that within all network stakeholders. This work was based on previous publications from the author (Mendez Mena et al., 2018; Mendez Mena & Yang, 2018, 2020) that included the appropriate permissions from the original publishers.

1.2 Scope

Recently, researchers have turned their attention to the applicability of existing blockchain protocols, as well as novel definitions, to other areas besides the original conceptualization of the technology, captured by different surveys and reports (Conoscenti, Vetro, & De Martin, 2016; Puthal, Malik, Mohanty, Kougianos, & Yang, 2018; Underwood & Sarah, 2016; Zheng et al., 2018). Moreover, the community has also started to dig into the suitability of blockchain properties to address security-related challenges for the IoT (Alphand et al., 2018; Conoscenti et al., 2016; Dorri, Kanhere, Jurdak, & Gauravaram, 2017; Gupta, Shorey, Kulkarni, & Tew, 2018; Kshetri, 2017). However, low-tier or consumer-based devices have not received the same notice even though it is estimated to be the largest category of IoT devices being used (Gartner, 2017).

Therefore, the purpose of this document is to develop and simulate a blockchain-based security framework that addresses security challenges for IoT devices functioning at the home-consumer level.

1.3 Significance

Over recent years, IoT devices and applications made their way to different areas, including homes, where their advantages and constraints were brought together. Most common IoT vulnerabilities include insecure web interfaces, insufficient authentication, insecure network services (prone to DoS attacks), privacy concerns (Yeh, 2016), insufficient security configurability, insecure software, and poor physical security according to Bertino and Islam (2017). In addition, IoT's principle of keeping a constant and ubiquitous operation, in addition to their weak security features and almost nonexistent technical maintenance, have made them "advantageous for creating botnets" (Kolias, Kambourakis, Stavrou, & Voas, 2017, p. 83). Moreover, Cui and Stolfo (2010) published an study that highlights the vulnerability of exposed IoT devices over the internet even to basic port scanning over well-known ports. The results found over 540,000 "things" that could be accessed by using default credentials. Costin, Zaddach, Francillon, Balzarotti, and Antipolis (2014) found that around 2,000 devices included backdoors, such as hard-coded telnet passwords, after analyzing the firmware of 32,000 embedded devices. Their study included home routers, which add other security vulnerabilities and software flaws that increase their probability of getting affected by common cyber attacks, backed by Karamanos (2010) results. For home users, the cost to manage smart home and network devices and IoT devices' proneness to be compromised place a burden over consumers that even increases the risk of exposure (Yiakoumis, Yap, Katti, Parulkar, & McKeown, 2011).

Known vulnerabilities and poor preventive measures for IoT devices led to Mirai botnet in 2016, which has been considered as "one of the most potent Distributed-Denial-of-Service (DDoS) attacks in history" (Kolias et al., 2017, p. 80). The Mirai botnet was able to pull over 1.1 Terabytes Per Second (Tbps) of TCP SYN requests to the French-based internet service provider OVH by using over 400,000 compromised devices that included webcams, DVRs, routers, etc... Mirai used a simple attack vector, it scanned the internet over port 23 and 223, used hard-coded 62 username-password pairs, and performed a brute-force attack to gain admin access. Once the malware gained control of the device and established communication with its command-and-control (C&C) center it started a General Routing Encapsulation (GRE), Transfer Control Protocol (TCP), and Hypertext Transfer Protocol (HTTP) flooding attacks on specific targets to bring them down. The original Mirai botnet and other variations are still found over the net and capable of infecting other vulnerable devices despite the InfoSec community's warnings of keeping unprotected and susceptible devices fronting the Internet (Kolias et al., 2017).

In summary, the risk for the IoT has increased, but the protective measures are thought not to be enough to deal with the current cyber security status. The challenges exposed are not trivial to define and they might be even more challenging to solve. IoT solutions that rely on legacy centralized systems are still prone to single-point-of-failure challenges, require costly dedicated infrastructure and support, and suffer scalability issues. Therefore, it exists the requirement to develop alternative solutions that respond to current challenges and needs from the different IoT tiers. As of now, cyber threats and attacks are considered as a burden that is taken by end users and their service providers (SP) (Yan, Kantola, & Shen, 2011). Therefore, it surfaces the requirement to reduce cyber risks at the home and SP level by acting proactively on emerging indicators of compromise (IOC) that have been validated by the network in real-time. The proposed framework objective was to offer near real-time (NRT) containment of network-based IOCs via a consortium blockchain network.

1.4 Research Question

The fundamental question and sub questions that define the study were the following:

1. Is it technologically viable to use blockchain protocols to develop a security framework for IoT devices and home networks?
   (a) How current network implementations behave under the referenced blockchain-based security deployment in terms of resource availability?
   (b) What are the security implications (user's network resiliency, and reliability) of implementing the proposed framework for users and service providers?

These questions were aimed to be answered in the following way: Research question one on chapter five, question (a) and question (b) on chapters three and four respectively.

1.5 Assumptions

The following assumptions were made for the current study:

- There exists a requirement to secure consumer-based networks and internal, non-mobile, IoT devices designed for home use.

- Network simulations in the study resemble production internet service providers' network, the network is designed and implemented correctly, and the network devices interact as expected.
- During simulations and throughout data collection, that all blockchain parties behave correctly under the rules and algorithms determined by the Ethereum protocol, and more than half of the users are trustworthy and legitimate.
- Simulations of security threats mirror known network-based attacks.

1.6 Limitations

The following limitations were inherent to the study:

- Simulations are restricted to the software and hardware capacity of the equipment utilized.
- Security resiliency and reliability of all network and blockchain components for unknown or not tested threats.
- There exists limited computing resources that sustain the private Ethereum network.

1.7 Delimitations

The delimitations for this study included:

- The intent of the proposed framework target home networks and IoT devices used in non-mobile applications.
- The blockchain-based suggested solution can only be considered as a proof of concept and has not been designed or developed for production environments.

1.8 Summary

During this chapter, the author provided the background, scope, significance, research questions, assumptions, limitations, delimitations, and definitions for the research project. In the next chapter, the author outlines blockchain technology, its history, limitations, evolution, and applications in different domains. The following chapter also includes a review of the Internet of Things (IoT) literature, security challenges, security requirements, and blockchain applications created to solve IoT security problems.

CHAPTER 2. REVIEW OF LITERATURE

2.1 Blockchain Technology and Its Evolution

In 2008, "Satoshi Nakamoto", either a person or a group of developers, published Bitcoin's white paper (Buterin, 2018) entitled "Bitcoin: A Peer-To-Peer Electronic Cash System" (Nakamoto, 2008) which introduced a decentralized peer-to-peer (P2P) electronic payment system that does not rely on financial institutions. Bitcoin offered a practical solution to the "double-spending" problem presented in digital currencies schemes (Crosby, Pattanayak, & Verma, 2016), such that all transactions are recorded on a public ledger which is validated by a consensus system based on strong cryptographic fundamentals (Mendez Mena & Yang, 2018). Bitcoin has experienced success, with a capital market of over 10 billion US dollars (Zheng et al., 2018). Moreover, its underlying technology, called "Blockchain" has captured researchers' and developers' attention during recent years.

The blockchain can be defined as an open distributed ledger that record digitally-signed transactions which are group-stored (in blocks) on a back-ordered hash list that is shared over a P2P network (Mendez Mena & Yang, 2018). Blocks are linked to each other by a pointer that contains the hash value of the previous block, which are attached in a linear and chronological order, Figure 2.1 shows a graphic representation. To decide which block should be appended next in the chain, as other blocks can be created simultaneously, Bitcoin introduced a consensus mechanism, also known as "Proof of Work" (PoW) (Crosby et al., 2016). The PoW consists on finding the correct random number (nonce) in the block's header that complies with the number of expected leading zeroes of the Secure Hash Algorithm-256 (SHA-256) hash value to be appended to each block (Christidis & Devetsikiotis, 2016).

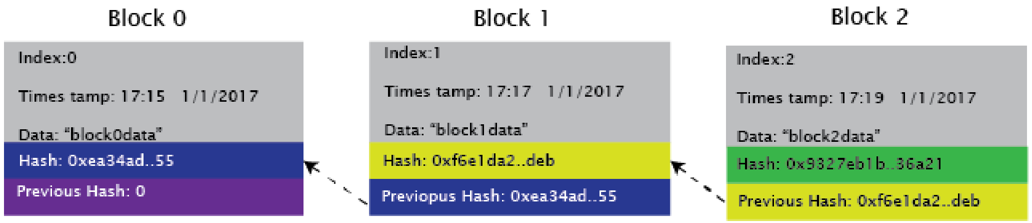


Figure 2.1. Blockchain representation (Mendez Mena & Yang, 2018)

The computational effort needed to obtain the right nonce is exponential to the number of zeroes anticipated, but it is simple (by one-way function definition) to verify by any other node in the network. Once a new block is generated and, therefore, broadcasted and verified by other nodes, the responsible party or "miner" is rewarded with Bitcoins (BTC), which also serves as an incentive to other network members to support the process (Karame & Ghassan, 2016). If two competing miners submit a candidate block at the same time (creating a "fork"), the consensus algorithm dictates that the nodes should accept the fork that shows the most considerable amount of work (solved by the next block). Therefore, besides making each block immutable and every transaction verifiable, it also increases the difficulty for an attacker to announce a fraudulent transaction as not only one block is needed, but all the subsequent blocks need to be recalculated, turning into a mathematical race with other well-behaved nodes (assumed to be the majority) to get it accepted (computationally expensive and almost improbable) (Crosby et al., 2016).

In summary, the blockchain provides byzantine fault tolerance (BFT), as it reaches consensus over a trustless environment, as well as decentralization, persistency, anonymity (not necessarily privacy), and auditability (Zheng et al., 2018). In short, the system provides confidentiality (for account management), grants integrity, and maintains availability based on its decentralized properties (Denial-of-Service (DoS) resistance) (Kareem, Bin Sulaiman, & Umer Farooq, 2018). The system is also resistant to Sybil attacks, in theory, as long as the rightful participants control at least 51% of the mining power (Raval, 2016).

2.1.1 Original Blockchain Limitations and Technical Response

Nevertheless, Bitcoin and its original blockchain present technical challenges and limitations that in some way complicate its adaptability on the road (Yli-Huumo, Ko, Choi, Park,

& Smolander, 2016). (1) Bitcoin's current maximum throughput is only seven transactions per second, which may limit its scalability if the number of users increases over time. (2) The time needed to complete a transaction is around 10 minutes (Kiayias & Panagiotakos, 2015), the time it usually takes to mine a block that relates to the number of zeroes required on the PoW, such latency makes the original blockchain unusable for immediate-sensitive applications. (3) Bitcoin's size of one block is close to one Megabyte (MB) limiting the number of transactions to 500, by the time Bitcoin reaches the throughput of its financial competitors, like VISA, it might experience bandwidth scarcity. (4) Current Bitcoin security relies on the assumption that to maintain the rightfulness of the system, the majority of the nodes in the network behave correctly. Karame and Ghassan (2016) listed three different practical attacks on Bitcoin's security by tampering blocks and transactions delivery. Sybil attacks were based on IP addressing control and fast payment meddling (for newer Bitcoin versions). Eyal and Sirer (2018) showed that minority mining pools could use a strategy called "Selfish Mining" to gain more than their legitimate share of mining rewards, which eventually can lead to more pools to apply the same approach and even being able to launch successful double-spending attacks. Additionally, software bugs have been found in Bitcoin's software that have derived in vulnerabilities, such as CVE-2010-5139 (integer overflow) (Park & Park, 2017). Finally, (5) Bitcoin mining consumes vast amounts of electrical power due to its trial-and-error strategy to find the nonce to provide PoW. In financial terms, around 15 million US dollars per day are needed to pay the electrical bill for the entire Bitcoin network (Yli-Huumo et al., 2016).

Bitcoin's limitations and flaws have created the necessity to look for alternatives or modifications to the original mechanisms to potentiate blockchain applicability and expand its realm. Original and consequent versions of the blockchain have been classified based on their potential activities. The blockchain community has come up with three categories (Swan, 2015): (1) Blockchain 1.0 groups currency exchange and financial-related applications, such as digital payment systems, led by Bitcoin and its technology (as explained previously). (2) Blockchain 2.0 is linked to contracts and comprehends the entire economic, financial, and market processes, such as stock and bond exchange, ownership, and public records (Hoy, 2017). Ethereum, launched in 2014, introduces a "blockchain with a built-in Turing complete programming language" (Wiederhold, Riva, & Graffigna, 2014, p. 13). Ethereum runs a distributed virtual machine or

"Ethereum Virtual Machine" (EVM) that runs "smart contracts" or self-enforcing computer programs (Atzei, Bartoletti, & Cimoli, 2017), Li, Jiang, Chen, Luo, and Wen (2017) considered Ethereum smart contracts as lightweight decentralized applications or dAPPs. The second version of the blockchain opens the door for application research in different fields. (3) Blockchain 3.0 deals with functions beyond finance and markets with functioning applications on government, science, health, technology, and education (Crosby et al., 2016). The third version of the blockchain is capable of running full-blown dAPPs or smart contracts, which include automated agents (AA) or software that runs without human intervention and creates decentralized autonomous organizations (DAO), where artificial intelligence systems make decisions and humans sit on the edges of the structure (Raval, 2016). Besides virtual computational features and automated enforcement, newer versions of cryptocurrencies with their respective blockchain modification address original flaws or limitations found in Bitcoin. New alternative coins or "altcoins" improve (1) throughput, (2) block interval time, (3) number of transactions per block, and (4) the consensus algorithm has been adjusted for security and efficiency purposes, such as the energy-friendly Proof-of-Stake (PoS) consensus method which requires fewer CPU cycles for mining and its reward system is based on the node coin balance rather than its computing power. Table 2.1 shows a quick comparison of some of the most relevant cryptocurrencies/blockchain systems at the moment, that includes information of practical tolerance to malicious nodes based on the security analysis of Zheng et al. (2018), Bartoletti and Pompianu (2017), and Kiayias and Panagiotakos (2015).

Table 2.1. *Blockchain comparison from Zheng et al. (2018), Bartoletti and Pompianu (2017), and Kiayias and Panagiotakos (2015)*

System	Block Size	Block Interval	Consensus Protocol	Energy Saving	Practical Tolerated Adversary Power
Bitcoin	96 GB	10 min	PoW	No	<25%
Litecoin	16.55 GB	2.5 min	PoW	No	<49%
Dogecoin	13.93 GB	1 min	PoW	No	<47%
Ethereum	17-60 GB	12 sec	PoW	No	<25%
Tendermint	10 GB	5 sec	BFT PoS	Yes	<33%

2.1.2 Blockchain Current Challenges

Although recent versions of the blockchain provide solutions to the constraints displayed with Bitcoin they also present new concerns. The nature of the blockchain, as a public ledger, even after new releases of the protocol, all transactions are public and in many cases users' activities are traceable. However, one-time accounts, one-time private keys for each transaction, and the use of transactional "chaffs" can help to protect against data leakage and improve privacy preservation (Li et al., 2017). Cruz, Peters, and Shevchenko (2015) proposed a framework for building smart contracts that safeguard privacy, consisting of a compiler named "Hawk" that translates the script into a cryptography-based protocol. Smart contracts, as computer programs, can also be used by malicious entities that can ease information leakage that includes confidential information and private keys, as well as use scripts for fraud and other crimes (Li et al., 2017). Additionally, smart contracts present vulnerabilities based on their functionality and technical conception. Atzei et al. (2017) described a vulnerability on auto-invoking contracts during a "fork" as its running state might be reverted and therefore undetermined. Also, described an attack on a time-sensitive contract used by a malicious miner, with stake in the outcome of the transaction that manipulates its execution. The study also included a recreation of a DAO attack in which the adversary takes advantage of a glitch of withdrawal functions, after fallback, to steal funds. Li et al. (2017) published four different bugs with potential security risks, which include but are not limited to (1) transaction-ordering dependence, (2) time-stamp dependence, (3) mishandled exceptions, and (4) reentrancy.

Nevertheless, the potential of the blockchain permits the development of applications that attempt to address security problems. One of the strongest points of the blockchain is the ability to provide data integrity relying on sound cryptographic properties, plus, its natural perception of time (Cruz et al., 2015) permits the expansion of services to other areas, in special security. Christidis and Devetsikiotis (2016) divulged the "out of the box" benefits of the blockchain beyond financial applications:

- Decentralized fault-tolerant P2P network.
- Consensus practical.

- Transparent, verifiable and auditable.
- Non-repudiation enabled.
- Predictable trustless participation.

Puthal et al. (2018) added to the list data immutability, and data authentication, which provide data security as a result. Tapscott (2018) even considered, due to the same arguments, blockchain technology capable of securing tracking, not only of financial activity but also of "virtually everything of value" (p. 5). However, not all security solutions are suitable to be replaced or complemented by blockchain applications, Puthal et al. (2018) described a scenario where a distributed ledger application could be utilized for security purposes, which is characterized by (1) different parties that transact through a third party, (2) the third party is not completely trustful, (3) the priority is to validate transactions and a system that provides data authenticity, and integrity is prime, (4) a tradeoff between integrity over confidentiality and performance can be tolerated, and (5) it is not time-sensitive (although evolutions of the blockchain significantly improved transaction rate and block size). Additionally, Wessling, Ehmke, Hesenius, and Gruhn (2018) advocated for a comprehensive engineering approach before the blockchain can be integrated into different solutions. With or without previous considerations, there are already security applications based on blockchain technology that includes data storage (Raval, 2016), protected health information (PHI) data access (Hoy, 2017), data control (Zyskind, Nathan, & others, 2015), distributed denial of service (DDoS) defense (Rodrigues, Bocek, & Stiller, 2016), breeder document protection (Buchmann, Rathgeb, Baier, Busch, & Margraf, 2017) and the Internet of Things (IoT) security (Puthal et al., 2018). In summary, the blockchain has the potential to solve security problems endorsed by its real-world practicality as well as its cryptographic soundness, however, a detailed analysis and comprehension of the security problem to resolve should exist as well as the appropriate testing, and verification before deployment.

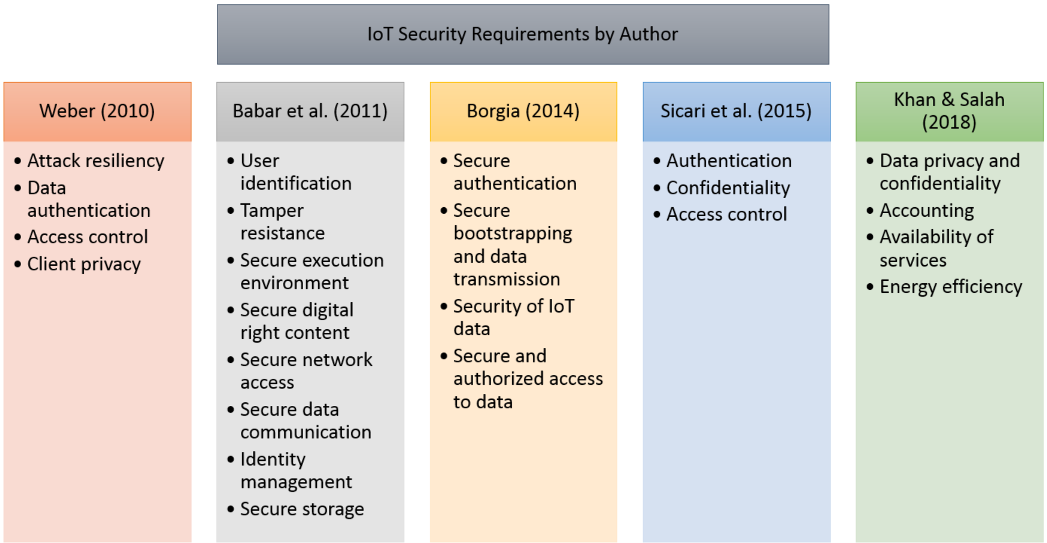
2.2 The Internet of Things

The Internet of Things (IoT) can be considered as a ubiquitous network of networks that comprehend a conglomerate of devices that provide different type of services (Oracevic, Dilek, & Ozdemir, 2017). Logically, it can be viewed as a group of smart devices that interact with each other to achieve a common objective (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015). These devices are interconnected providing and retrieving data, with intelligent responses that trigger actions (Mendez Mena et al., 2018). Lately, the popularity of the IoT has surged while many other IoT devices are being deployed globally and, therefore, the amount of data has surged as well. In fact, Gartner (2017) predicted that by 2020 the number of IoT devices would increase to 20 billion, moreover, Forbes (2016) estimated a data exchange greater than 40 Zettabytes (ZB) over the same period. Such important increase has created a gap between security and the IoT service breadth. Sivaraman, Chan, Earl, and Boreli (2016) concluded that business pressure, cost savings, and a revenue-centric model force a rush-to-market approach, Wurm, Hoang, Arias, Sadeghi, and Jin (2016) called it “short time to market (TTM)” (p. 519) , which enables security flaws. He et al. (2018) blamed flawed software-development practices, poor management of information streams, and burdensome patching process for devices in production stages. Additionally, the constrained nature of IoT devices with limiting power, memory and computing power exacerbates the situation as it contradicts legacy resource-exhaustive security solutions (Mendez Mena & Yang, 2018). Besides their own and the inherited flaws of traditional computer networks (Khan & Salah, 2018), attackers have also paid more attention to the IoT given the considerable amount of sensitive data processed without proper security controls (Lohachab & Karambir, 2018), which makes the situation even more compelling.

2.2.1 IoT Security Challenges

Security researchers have analyzed different perspectives to understand the current situation and define the existing challenges for the IoT. (Bertino & Islam, 2017, p. 78) listed common problems found in IoT devices that include: “Insecure web interfaces, insufficient authentication, insecure network services, poor privacy controls, insufficient security configurability, insecure software, and poor physical security."

Mahmoud, Yousuf, Aloul, and Zualkernan (2015) provided a more organized view of IoT challenges by classifying them in regard of its architecture: At the perception layer, wireless communications interference, interception, or alteration (replay attacks), as well as physical security must be considered. The network layer is susceptible to DoS, eavesdropping, and weak authentication are major concerns. Lastly, the application layer might experience complications from the heterogeneous nature of IoT as the lack of governing policies and standards complicates interaction, such as the utilization of contrasting authentication mechanisms. Lohachab and Karambir (2018) specified weak passwords, dissimilar storage and data processing methods, as well as flawed security controls and insufficient filtering capacity as the main reasons for IoT devices to miscarry privacy, trust, confidentiality, identity attestation, and access enforcement. Zhang et al. (2014) detailed faulty identification integrity, lack of global authentication schemes, poor privacy strategies (data collection policies and data anonymization), insufficient lightweight cryptographic solutions, deficient software development practices and software analysis constraints, as well as malicious software, complicates the IoT security panorama. Pacheco and Hariri (2016) added Internet network extension (from mobile, non-IP, sensor to cloud and fog computing), multiple entry points and domain diversity (on ownership, policy and connectivity) to the list of obstacles. Yu, Sekar, Seshan, Agarwal, and Xu (2015) included inadequate perimeter defenses, host-based detection mechanisms, and patching processes adapted to the IoT world as key dimensions that need to be addressed. Finally, Oracevic et al. (2017) summarized aforementioned IoT security issues into two main topics: Data and privacy protection. In summation, the security breadth has expanded but still the available resources are not sufficient to cope with the ongoing environment. The challenges exposed are not trivial to define and they might be even more difficult to solve. From the literature, consensus is still needed along with prioritization before the community can advocate for action.



IoT Security Requirements by Author

Weber (2010)	Babar et al. (2011)	Borgia (2014)	Sicari et al. (2015)	Khan & Salah (2018)
• Attack resiliency • Data authentication • Access control • Client privacy	• User identification • Tamper resistance • Secure execution environment • Secure digital right content • Secure network access • Secure data communication • Identity management • Secure storage	• Secure authentication • Secure bootstrapping and data transmission • Security of IoT data • Secure and authorized access to data	• Authentication • Confidentiality • Access control	• Data privacy and confidentiality • Accounting • Availability of services • Energy efficiency

Figure 2.2. IoT Security Requirements by Author

In any case, before solutions can be sketched, basic security requirements for the IoT should be determined, therefore, some researchers have established different conditions secure IoT devices should comply with. Figure 2.2 lists different requirements set by Weber (2010), Babar, Stango, Prasad, Sen, and Prasad (2011), Borgia (2014), Sicari et al. (2015), and Khan and Salah (2018). Lately, Samaila, Sequeiros, and Correia (2018) provided a more detailed and organized set of security requirements based on the IoT architecture that added to previous demands: Sensing [lightweight encryption, and anti-collision algorithms], network [secure routing, network encryption mechanisms, and attack detection/prevention] and application [secure cloud environment, antivirus software, security education].

However, it is more accessible to list demands than to develop solutions, some of the authors referenced above have overlooked existing limitations of constrained devices, which in some cases need to relate to external dedicated devices to provide a feasible resolution. Other authors made broad requirements that involve integral answers or “silver bullets” that so far have not been part of the security domain. Table 2.2 shows a recap of IoT security issues and author-concerted requirements based on its architecture.

Table 2.2. *IoT security challenges and concerted requirements by architecture layers*

IoT Layer	Security Challenges	Security Requirements
Perception		
	• Poor Physical Security	• Tamper Resistance
	• Communication Jamming	
	• Lack of Confidentiality and Integrity	
Network		
	• Insufficient Authentication	• Authentication & Access Control
	• Insecure Network Services	• Confidentiality & Integrity
	• Denial of Service	• Availability
	• Eavesdropping	• Attack Prevention/Detection
	• Deficient Filtering Capacity	
	• Scarce Lightweight Crypto	
	• Network Heterogeneity Extension	
	• Multiple Entry Points	
	• Inadequate Perimeter Defenses	
Application		
	• Insecure Web Interfaces	• Privacy
	• Poor Privacy & Security Controls	• Secure Execution Environment
	• Insufficient Client Security Configurability	• Secure Cloud Environment & Storage
	• Insecure Software	
	• Lack Governance and Standards	
	• Weak Passwords	
	• Incompatible Data Processing Methods	
	• Faulty Software Development Methods	
	• Constraint Software Analysis	
	• Malware	
	• Poor Patching Processes	
	• Unavailable Host-Based Detection	

2.2.2 Existent IoT Security Solutions

Based on the requirements exposed previously it is possible to formulate and analyze security solutions to the problems IoT has been struggling with. Examining the solutions at the perception layer, specifically to address tamper resistance, there has been studies that address jamming over wireless networks, such as the work presented by Noubir and Lin (2003); Xu, Trappe, Zhang, and Wood (2005); Xu, Wood, Trappe, and Zhang (2004) that can be applied to current IoT infrastructure as those rely on signal strength, packet delivery efficiency, correcting codes, and change of frequencies to avoid interference. Same for Sybil and spoofing attacks at this layer as exposed by Chen, Trappe, and Martin (2007); Demirbas and Youngwhan Song (2006); Li and Trappe (2006); Xiao, Greenstein, Mandayam, and Trappe (2007). Also, there are some other proposed solutions for securing physical interfaces and unverified network modules (OWASP, 2014).

At the Network layer, authentication and access control solutions have received important amount of attention from security researchers, as different approaches have been presented over the last few years. For instance, Granjal, Monteiro, and Silva (2010) proposed compressed versions for Authentication Header (AH) and Encapsulating Security Payload (ESP) mechanisms for Wireless Sensor Networks (WSN), where the authors evaluated different encryption techniques to find one suitable for limited energy requirements, such as Secure Hash Algorithm-1 (SHA-1), which by the way is no longer considered secure. Raza, Duquennoy, Höglund, Roedig, and Voigt (2014) proposed a similar approach for IPSec suitable for IPv6 Low-Power Wireless Personal Area Networks (6LowPAN) to reduce packet size that contradictory produces power overhead and increased response time. Mahalle, Anggorojati, Prasad, and Prasad (2013) introduced a new method for authentication and access control called Identity Authenticaiton and Capability based Access Control (IACAC) that genereates keys through Elliptic Curve Cryptography (ECC) where devices are mutually authenticated for communication and access to prevent man-in-the-middle and replay attacks. Kothmayr, Schmitt, Hu, Brünig, and Carle (2013) suggested an end-to-end security lightweight method that uses two-way authentication with public and private keys, in which an access control server stores access credentials for network users, a certificate authority (CA) is needed. Huang, Xiang, Bertino, Zhou, and Xu (2014) introduced a password-based authentication method that uses smart cards and biometrics that are registered at a database that also includes a back-up stand-alone solution when the central server is not available, similar to the proposal from Amin, Kumar, Biswas, Iqbal, and Chang (2018), in which the main purpose was to secure distributed cloud environments with low computational costs.

Bohli, Skarmeta, Victoria Moreno, Garcia, and Langendorfer (2015) proposed a distributed data access scheme that includes a distributed Kerberos authentication application to secure communication channels between IoT devices and the cloud by the use of crypto-generated keys within the Constrained Application Protocol (CoAP). Park and Kang (2015) proposed an inter-device authentication protocol and key-distribution scheme where the nodes are involved in the key assignment process instead of a central server. He et al. (2018) introduced a context-based authentication and access control framework based on the premise that IoT devices are managed by different users at the same location.

Additionally, as part of access control and permissions policy, trust should be considered as a key element between users/owners (if device usage is transferred) or between devices. Xie and Wang (2014) presented an approach for inter-system mutual trust that creates a centralized token-based access control framework based on item levels. Also, Tragos et al. (2016) proposed a trust model that calculates the trustworthiness of an IoT device based on communication, security, data-based criteria, relationships, location context, and reputation.

Confidentiality and Integrity literature seems to be mature as well, for instance, back in 2009, Riaz, Kim, and Ahmed developed a security framework to secure LoWPANs that contains modules for secure neighbor discovery, authentication and data encryption based on ECC. Brachmann, Garcia-morchon, and Kirsche (2011), presented a end-to-end security solution for CoAP that integrates also with HyperText Transfer Protocol (HTTP) using Transport Layer Security - pre-shared key (TLS-PSK). Doukas, Maglogiannis, Koufi, Malamateniou, and Vassilacopoulos (2012) proposed a conceptual design that provides data encryption and integrity (as well as authentication) by the use of public key infrastructure (PKI) at the IoT gateway level, as those devices have more robust computational resources that common IoT devices do not. Peretti, Lakkundi, and Zorzi (2015) suggested another framework to provide end-to-end security that includes lighweight versions of CoAP, Datagram TLS (DTLS) and 6LoWPAN over TinyOS. Kumar, Kumar, Budhiraja, Das, and Singh (2016) proposed a Lightweight encryption algorithm that utilizes a symmetric key algorithm of five rounds that uses a 64-bit key to encrypt a 64-bit block cipher. Das and Das (2016) introduced a hybrid method that combines cryptography and steganography techniques to achieve confidentiality and data integrity, respectively, between home and cloud servers. More recently, Aman, Sikdar, Chua, and Ali (2018) introduced a two-step approach to validate IoT data integrity that includes a random time hoping sequence, using shared secrets between the data server and the IoT device, and then creates validation information using a lightweight random permutation algorithm.

The literature that covers availability solutions for the IoT is not as extensive as prior requirements described above. Misra, Krishna, Agarwal, Saxena, and Obaidat (2011) proposed a service oriented architecture that aims to prevent DDoS attacks for IoT by using Learning Automata (LA) concepts which optimized packet examination problem for recognition of malicious ones, it is composed of various phases for detection, identification, and defense, where different thresholds are defined based on resource availability. A different approach is suggested by Jerkins (2017), in which it tried to catalog Mirai-vulnerable IoT devices to motivate administrators to remediate the problem. Rajagopalan, Jagga, Kumari, and Ali (2017) proposed to move the burden to IoT gateways in the Fog layer so authentication and authorization methods can be run appropriately.

Attack prevention and detection methods for the IoT are scarce, for instance, Liu, Zhang, and Zhang (2013) presented a dynamic defense architecture that utilizes Artificial Immune System (AIS) adaptation to detect attacks through an IoT gateway and an attached monitoring server. Yu et al. (2015) proposed network-based security architecture that relies on security gateways that monitor and control the context of IoT devices to generate a global view of the network enforce policies that include internal interactions. Sivaraman, Gharakheili, Vishwanath, Boreli, and Mehani (2015) suggested a network-level monitoring solution capable of detecting malicious behavior that interact dynamically with cloud-based Software Defined Networking (SDN) to implement security rules at the IoT gateway. Pacheco and Hariri (2016) presented an IoT framework that contains an Anomaly Based Analysis (ABA) - Intrusion Detection System (IDS) to detect irregularities at the sensor and network layers, it used comparative methods to determine deviations between the Euclidean distance and reference models determined by the ABA.

In addition, there are a few solutions involved in the attack prevention domain that could be used as compliment to the applications described previously to provide reliability and scalability to the scheme. For instance, Sharma, Singh, Jeong, and Park (2017) suggested a distributed SDN network to maintain consistency between controllers as well as to keep a secure interaction between them to apply security network controls and threat prevention to IoT networks. Additionally, Collen et al. (2018) published a conceptual reference architecture that involves network data flow analysis for context information to develop a risk assessment in real time and traffic control at the IoT Gateway. The platform uses Blockchain and Smart Contracts to provide data assurance and code integrity that can be used to distributively share information with other IoT gateways.

At the Application layer some of the security solutions crafted to address privacy, execution, and cloud environments also interact with the other two layers or with external or non-technical approaches. That is the case of user-level privacy and data sharing as different controls are needed from a governance point of view. Nevertheless, policies must adapt to the dynamic IoT environment and technology should be able to provide some tools to guarantee the application and the enforcement of this policies (Sicari et al., 2015). In regard of data privacy (at motion or at rest), solutions at other layers, such as encryption techniques as well as authentication and access control methods are required to comply with this requirement.

In order to assure a secure execution environment, besides the security applications described on previous layers, can be guaranteed by testing how IoT systems would react to a different set of attacks and consequent failures that would risk confidentiality, integrity, or availability. That is the approach Strielkina, Kharchenko, and Uzun (2018) and Kolisnyk and Kharchenko (2019) have taken to propose Markov's models to better understand the outcome of simulated attacks on vulnerabilities or on availability (respectively) on each of the components of the IoT infrastructure without harm.

The IoT has found in the cloud a place to outsource storage and computing capabilities that is not able to support within its limited hardware that has brought IoT's intrinsic threats and security problems into the new domain, which in some ways can be addressed by the methods presented previously. However, current research has been mostly compartmentalized and there has not been numerous efforts to address challenges as a whole (Roman, Lopez, & Mambo, 2018). Nevertheless, Bhattasali, Chaki, and Chaki (2013) published a framework to secure communications with the cloud, however, it needs trust to be established in the first place. Zhou, Cao, Dong, and Vasilakos (2017) proposed a secure packet forwarding and privacy preserving framework for cloud-based IoT (viewed as a single environment) based on threshold credit-based incentives (TCBI) mechanisms and symmetric homomorphic mapping (SHM) encryption for packet forwarding and one-way trapdoor permutation to preserve privacy.

In summary, IoT solutions that rely on legacy centralized systems are still prone to single-point-of-failure challenges, require costly dedicated infrastructure and support, and scalability issues. However, those provide reliability as they have been subjected to scrutiny of the security community over time, therefore, their limitations and flaws are acknowledged so they can be utilized in the correct context.

2.2.3 Blockchain Security Solutions

On the Blockchain side, there exists a significant number of publications that address authentication, and access control. For instance, Ouaddah, Abou Elkalam, and Ait Ouahman (2016) and Ouaddah, Elkalam, and Ouahman (2017) proposed a blockchain-based access control framework, called FairAccess, that enables a decentralized access control manager to grant, delegate, and revoke access to allow users to have full control over their data and consequent privacy by the use of smart contracts, wallets and access tokens, where the control and Bitcoin-enabled blockchain processes are enforced at IoT gateways. Shafagh, Burkhalter, Hithnawi, and Duquennoy (2017) published a new distributed access control framework to secure data sharing and storage in the cloud, it uses Bitcoin's blockchain to maintain an auditable access control ledger to provide secure key distribution for data stream encryption. Ourad, Belgacem, and Salah (2018) introduced an authentication model via Ethereum blockchain, smart contracts, and tokens to allow a one-time login to interact with different IoT devices, that run instances of the blockchain, to verify identities over a public network. Novo (2018) presented a new decentralized access control architecture that operates in a single smart contract where IoT devices interact with the blockchain through management hubs that also interface with a public network of full blockchain nodes controlled by the contract. Additionally, Hammi, Hammi, Bellot, and Serhrouchni (2018) presented a decentralized authentication mechanism running on top of a public Ethereum network that enables virtual secure zones enforeced by smart contracts, where IoT devices can communicate safely. Both, client/server and blockchain solutions attempt to solve inherited IoT problems through similar cryptographic fundamentals and lightweight adaptations of models that have worked on other instances. However, blockchain-based solutions also seek to solve legacy client/server problems such as third-party availability and authenticity, scalability, and availability. Nevertheless, Blockchain-based approaches are usually concepts that in some cases offer light test implementations that need additional work before real-world introduction.

Blockchain-based publications on confidentiality and integrity are not as extensive as their counterparts, however, blockchain applications on their own provide naturally integrity as that is considered a strong characteristic of these systems. Nevertheless, Liu, Yu, Chen, Xu, and Zhu (2017) presented a data integrity as a service model for IoT-cloud interactions that can be verified by data owners and consumers without a third-party auditor that runs on top of a private Ethereum network. Blockchain applications cannot offer data confidentiality directly as its publicly-available attributes are antagonistic, and should rely on other solutions, however, it can assist providing a platform to verify identities and create a secure exchange between verified IoT entities. On the availability area, blockchain approaches are not sufficient either, Boudguiga et al. (2017) proposed an infrastructure availability framework by using the blockchain to maintain IoT devices patched with validated software signed by manufacturers via a web portal that interacts with the blockchain network and publicly-available IoT devices, and therefore, improve its availability. As different approaches are taken to prevent IoT availability issues there exists the possibility to combine methodologies to achieve a more resilient system.

Novel applications based on the blockchain still need time and research to acquire a “solution” status. As seen previously, blockchain technologies can administer side services to provide resiliency or to enhance existing security to the desired environment, which in most cases can be adapted within other architectures as long as the requirements, needed to conduct a successful blockchain implementation (previously described), are met.

2.2.4 Blockchain Security Solutions for the IoT

2.2.4.1 IoT Service Categorization

In order to review different security applications, it is worth to classify IoT devices by their operation domain as different requirements might be obtained by the service they were meant to offer. Ouaddah et al. (2016) suggest classification by three main different domains, Boudguiga et al. (2017) added a fourth one:

1. Personal & Home
2. Government & Utilities
3. Enterprise & Industry
4. Intelligent Transport Systems (from Boudguiga et al. (2017))

It is possible now to allocate current IoT market offerings in to the described categories. For instance, Healthcare and SmartHome devices fall under the Personal & Home category, SmartCities and Smart Grids under Government & Utilities, manufacturing-purposed devices, or Industrial Internet of Things (IIoT) solutions, under Enterprise & Industry, and autonomous motor vehicles below Transport Systems. Additionally, Ouaddah et al. (2016) listed some of the requirements for each one of the domains, for example, Personal & Home devices seek for privacy practices, Government & Utilities call for scalability and collaboration features and Enterprise devices demand authorization controls and availability, which intuitively can be assigned for IoT transport systems as well. Also, Tschofenig, Arkko, Thaler, and McPherson (2015) classified IoT devices operation by their communication patterns, which are not mutually exclusive: (1) Device-to-Device, (2) Device-to-Cloud, and (3) Device-to-Gateway.

2.2.4.2 Blockchain Operational Categorization

Blockchain technologies can also be organized by their operation type: (1) Public, (2) Consortium, and (4) Private (Buterin, 2015). Public blockchains are accessible by anyone over the Internet, users can interact freely with it and secured by monetary compensation. Consortium blockchains are maintained by a "pre-selected set of nodes" (Buterin, 2015, p. 1) where read rights may be public or not, and private blockchains are fully restricted systems with constrained rights to read, generally belonging to a specific organization. Table 2.3 compares the three types as the consensus method, the efficiency, and the security differ within each other.

Table 2.3. *Blockchains by operation type*

Attribute	Public Blockchain	Consortium Blockchain	Private Blockchain
Access	Unrestricted	Pre-selected set of nodes	Restricted (One Organization)
Read Rights	Public	Public or restricted	Public or restricted
Security	Difficult to tamper	Might be tampered	Might be tampered
Consensus	Permissionless	Permissioned	Permissioned
Efficiency	Low	High	High

As security, or chain immutability, relies on the number of well-behaved users, public blockchains are difficult to tamper as the number of malicious nodes must be majority (theoretically), therefore, private and consortium chains with limited number of nodes can be tampered with more ease, although, their security also relies on their restriction capabilities (Gramoli, 2016). The consensus process can also variate as consortium and private blockchains restrict and certificate participation, unlike public ones where anyone can enroll. Efficiency deals with transaction throughput (latency) and power consumption (Zheng et al., 2018). Blockchain applications might differentiate as well by the platform used (Bitcoin, Ethereum, Tendermint, Custom, etc.) and consequently consensus methodology (PoW, PoS, BFT, Proof of Authority (PoA), etc.).

2.2.4.3 Blockchain-Based Security Applications

There are blockchain security applications for the IoT that cover fundamental security operations or protocol enhancements that could be used in different domains. For instance, Ouaddah et al. (2016) introduced a distributed access control framework, that is composed by two layers, the first one manages the access control policies that communicate with other organizations, and the second one comprehends IoT devices that rely on their blockchain-enabled gateway, that enforces the access control policies. In this case, a semi-centralized approach is used as IoT equipment do not own the computing resources to apply rules by themselves, according to the authors. The proof-of-concept runs over Bitcoins's blockchain and utilizes wallet interfaces to relate to users, which means currency is needed to run the application and limits its affordability and may become a burden if the number of nodes grow, nevertheless, the integrity of the transactions are safeguarded by Bitcoin's entire capability.

Boudguiga et al. (2017) proposed to use the blockchain to keep diverse IoT devices updated and to check patch integrity, the objective is to provide a highly available distributed network that can provide the required patches to outdated IoT devices. The IoT devices interact with the blockchain directly to reach the validated software that rests over other file servers with more computing capacity. The prototype version runs Multichain, an open-sourced private blockchain enabler that is a modified protocol of Bitcoin's technology. Even though blockchain main features may provide the security safeguards offered, the publication does not show efficiency nor security analysis data. Additionally, IoT devices are emulated by Rasperry Pi minicomputers that not necessarily reflect adaptability or capacity of current market offerings. Also, the update network works on top a private blockchain that if no security controls are enforeced properly can be overwhelmed by malicious nodes.

Lee and Lee (2017) published a similar approach to provide validated firmware to constrained devices connected to a custom-made private blockchain where the firmware updates are distributively stored and shared via a BitTorrent application (Peer-to-Peer (P2P)). The scheme is composed of verification nodes, that keep integrity information of the update files, vendor nodes (outside of the blockchain network) that store and share the software uniquely based on verification node information, and user nodes (IoT devices), that produce continual queries for new firmware updates. The document contains a detailed and formal explanation of each one of the roles, protocols, and structures used in the solution. However, the authors did not present a proof-or-concept nor simulation of any of the processes that difficult the analysis. Efficiency scrutiny is necessary as such data can tell how well intensive computing tasks take place on PoW miners, as well as the impact on constrained devices running blockchain operations, as the number of network members increase.

Shafagh et al. (2017) introduced an access control management solution for IoT devices that uses blockchain technology to provide secure data sharing protocol. The Bitcoin blockchain stores access permissions that are granted on a data-stream basis, which could be revoked at any time by the data owner. The IoT devices interact with the blockchain through the IoT gateway that also serves as a intermediary storage unit, that also caches recently used data. The paper includes thorough description of the blockchain and data storage process that include formal message definitions. The primary evaluation presented by the authors shows a slowdown compared to Amazon's S3 storage service that increased with the inclusion of more nodes. Further testing and supporting data is needed for blockchain mining efficiency suitability from a proof-of-concept implementation.

Ourad et al. (2018) came up with a one-time authentication scheme built on top of a public Ethereum smart contract that determines resource accessibility. Once the user is authenticated, and granted an access token, she/he can interact with the IoT device (running an Ethereum lightweight client) by any communication method during the authorized time or until revoked. Initial testing showed resiliency against replay, man-in-the-middle (MITM) attacks, and malicious packet injections, although cryptanalysis is missing. It also shows ease of use, as the end user needs to make a single request to maintain data accessibility. In terms of blockchain efficiency, even though the study did not present data, seems reliable as mining is not needed as a Proof-of-Authority (PoA) protocol is used. Nevertheless, the solution needs actual currency (gas) to run instructions determined in the contract, which can mean an important financial stress over the system owners when more devices are attached. Also, the proposed platform requires blockchain-enabled devices to complete the authorization process, that in reality might be difficult to achieve as IoT manufacturers need to be involved.

Hammi et al. (2018) published a decentralized blockchain authentication system that creates virtual zones of trust, where IoT devices can communicate safely and external communication is restricted by a public smart contract. The blockchain is used outside the security zones and it is composed of a "master" IoT device that interacts with the blockchain for group creation and association requests, and "follower" IoT devices that run Ethereum client software. The authors presented efficiency analysis that include power consumption, financial costs, and transaction throughput that, even though, it shows feasibility arguments, it was not compared with other baseline implementations. The solution, as it works on top of public Ethereum network, inherits its robustness (including its limitations) and security capabilities as well as provides different layers of protection, at first sight, for IoT devices against spoofing, replay, and message substitution attacks, although further analysis and testing is needed. However, public Ethereum transactions have a monetary cost, which is volatile and difficult to calculate over a time range, that may become a difficulty as more devices are added to the system. Also, IoT devices need to run Ethereum instances that require vendor intervention before it could be set under production.

Gupta et al. (2018) offered a new security model custom blockchain inspired after Bitcoin, that trades tokens instead of coins that are used to distribute voting power and limit transactions rate to prevent DoS attacks. The new protocol exchange additional messages that exchange authentication information as well as public keys to enable confidential exchange of data. Nevertheless, the publication lacks cryptoanalysis of the different exchanges as well as experimental data that confirms the operability of the protocols. Custom offerings for blockchain protocols need to present empirical evidence of their feasibility and reliability.

Wang, Dong, Li, Fang, and Chen (2018) proposed a custom blockchain security model for the IoT that utilizes an Inter-Planetary File System (IPFS) that queried transactions. The IoT devices interacted as nodes of the blockchain, that isolates their interface with external networks, as only validated and signed transactions are processed. The authors simulated a deployment that indicated excessive latency and low throughput as the number of nodes and transactions augmented, which might indicate performance problems if the solution is taken under more challenging situations. Additionally, the paper does not offer data nor analysis on device performance as IoT equipment actively interacts with the blockchain and the file system. However, the system is able to deliver security and decentralized capabilities that the blockchain protocol offers.

Alphand et al. (2018) presented an adaptation of the IoT architecture for end-to-end data transfer security published by Vučinić et al. (2015) and the IETF Internet Draft authored by Seitz, Selander, Wahlstroem, and Erdtman (2017) for authentication and authorization of constraint devices. The solution replaces third-party servers of mentioned approaches with a trustless authorization method based on token exchange over blockchain and private Ethereum smart contracts that contains and enforces access rights' policies. The data showed, after implementing the proof-of-concept (PoC) on top of the Ethereum private test network, response efficiency and acceptable latency on each of its services including the constrained device utilized as the computing burden was carried by servers with sufficient computing power. However, the PoC was deployed with a limited number of devices that would require additional testing as the transactions are increased by additional IoT devices, clients, and service nodes. Furthermore, the solution requires of adaptable IoT devices that can support a blockchain instance with sufficiency.

Under the Personal & Home category, Dorri, Kanhere, Jurdak, and Gauravaram (2017) presented a blockchain-based smart home framework (initially conceptualized in Dorri, Kanhere, and Jurdak (2017)), which might be applied to different domains as well. The framework involves three tiers that are included in a smart home environment, where IoT devices request or allow access to device data through a private blockchain maintained by a local miner that acts as the network gateway. Also, the solution includes cloud storage with a compatible service provider (SP), and an overlay network composed of clustered smart homes running a public blockchain system to connect different instances under a common administrator. The framework offers two different layers of protection that could contain spread attacks from or within the smart home. Additionally, it offers integrity of data transactions, management availability, confidentiality for data at rest, and computing resource efficiency as a custom blockchain instance is used that do not require PoW. Nevertheless, it requires IoT devices, service providers and data storage platforms to work under the same authentication and access control protocol, which may be difficult to accomplish, which also limits the implementation and testing of the proof-of-concept that ended up in a computer-based simulation. Lastly, running a novel customized private blockchain protocol might carry software vulnerabilities unless rigorous testing is applied.

Huh, Cho, and Kim (2017) proposed and IoT device management model that works on top of an Ethereum private network. The proposal used Raspberry Pi devices as home appliances meters that collect energy consumption data from different appliances and enforce consumption policies dictated in smart contracts, the blockchain stores public RSA keys and protect its integrity . Some of the data obtained from the meters is also stored in the blockchain based on the policies stated in the contract. The authors mentioned some of the limitations found in the Ethereum protocol that they need to address to increase functionality, such as transaction throughput and lack of lightweight clients suitable for constrained devices. Even though, conceptually, the solution seems to accomplish its objectives as it was implemented over a test network, the study does not present an efficiency nor security analysis, basic operational data is not available either. Also, a profound privacy analysis is needed to determine whether the data stored in the blockchain does not leak user identifiable information.

For Government & Utilities IoT devices, Mylrea and Gourisetti (2017) conceptualized a blockchain model for smart grids that aims to enhance the integrity and the trustworthiness of transactive energy data based on a public and decentralized ledger. Additionally, it analyses the potential of secure decentralized data storage as well as verification of transactions that a blockchain solution and smart contracts could offer. Moreover, the data distributed over a blockchain network could also be used to detect abnormal behavior or tampering attempts that could minimize the risks and improve the stability of the system. Also, it enables smart grids to decentralized payment systems and allow real-time trading based on actual energy consumption gathered from smart meters. Nevertheless, the publication offers only conceptual solutions to existing smart grids cybersecurity problems, such as resiliency, trustworthiness and data integrity preservation.

Under the Enterprise & Industry category, Liu et al. (2017) introduced a integrity-as-a-service platform that enables data owners and consumers and providers to verify IoT-generated data integrity under a decentralized environment. The data integrity system is controlled by a private Ethereum smart contract where clients, owners, and service providers can verify completeness of the data stored in the cloud. The data transfer process is possible through a P2P system relying on IPFS over secure Hypertext Transfer Protocol (HTTP). As intended, the solution leverages from the most prominent feature provided by a blockchain, integrity. The platform permits as well to avoid third-party auditors and provides availability. The system also allows to process payment to the cloud storage provides through the same Ethereum network that compensates honest miners for their verification services, which can be even more gratifying if the solution works publicly. Nevertheless, it requires client, owner and cloud service provider to support the same blockchain instance and custom made protocols. Additionally, further testing is needed over a larger network and monitor verification efficiency as published results over a limited environment showed considerable delays for blocks larger than 8 MB.

Sharma et al. (2017) proposed a multilayer network distributed architecture for enterprise environments. The solution uses the blockchain for network controllers to allocate network topology and traffic data to dictate policy rules for the software defined networking (SDN) management platform. The system learns common traffic patterns and reacts to abnormalities that interact with SDN and access control rules to block possible threats. The proposal strengths reside on its ability to adapt current technologies with fault tolerance distributed protocols without altering IoT composition and functioning that interact with a high-availability architecture. However, the solution works on top of a custom blockchain private network that might not offer the same robustness as major blockchain offerings. Also, addtional real-world testing and comparison studies are needed as the published simulation might not encompass all variables. Finally, due to its complexity and scope it is limited to organizations with the financial means to deploy.

Finally, for Intelligent Transport Systems, Dorri, Steger, Kanhere, and Jurdak (2017) published a decentralized security architecture for a smart vehicle environment based on a custom blockchain protocol. Smart vehicles or support services (i.e. smart devices, software providers, cloud services, etc.) connect to management nodes that comprehend a blockchain network that does not require proof-of-work computation but rather assigns block creation by schedule. Management nodes verify and broadcast signed transactions as it allows traffic only to and from an access control list composed of public keys generated from each IoT device or service. The authors suggest remote software updates, insurance data sharing and car sharing services as potential applications of the architecture. The proposed changeable protocol for public keys allows to maintain certain privacy assurance features that other blockchain IoT solutions have not addressed entirely. Also, as a private blockchain approach, it does not need extensive validation mechanisms that affect power and computer efficiency as well as providing a more restrictive environment, where access control could be enforced more strictly. Nevertheless, implementation on real scenarios might require a significant effort to deploy a compatible network with sufficient coverage for mobile users. Additionally, custom-made blockchain protocols need thorough testing and analysis before they can be part of a production environment.

Even though the number of IoT-Blockchain publications has increased significantly over the last three years almost by a factor of 20 (Web Of Science, n.d.), there are some IoT requirements that have not been completely satisfied. The number of publications suggesting blockchain solutions for authentication, access control, availability, integrity, privacy, cloud integration and storage for the IoT is relatively booming. On the other hand, prevention & detection, as well as secure execution environment initiatives did not receive the same attention as the previous ones. Additionally, as stated by Gartner (2017), the number of home-based and personal devices represent over the 50% of all IoT devices with a projection to almost 12 billion devices by the next two years, which makes it a primary focus of attention for businessman, researchers, and malicious actors. Such consideration intensifies the need to address security issues not only technologically but also from the policy standpoint.

2.3 Summary

In this chapter, the author provided a review of the literature relevant to the blockchain technology, the Internet of Things, its security challenges and proposed solutions that leverage on the blockchain to address IoT's requirements. Even though the results of the section establish the importance of and the relevance of the research questions proposed, none of them were able to provide a response. In the following chapters, the author presents his research compiled in two additional publications (Mendez Mena & Yang, 2018, 2020), as well as future writing plans.

CHAPTER 3. BLOCKCHAIN-BASED WHITELISTING FOR CONSUMER IOT DEVICES AND HOME NETWORKS

In the following chapter, the author summarizes the work published by the author of this document, Mendez Mena and Yang (2018), presenting blockchain-based security solutions for home networks and home IoT devices. The author relied on hardware implementations with known IoT “Smart Home” devices to create a practical testing environment. The numerical data obtained were subject to statistical analysis and compared to a simple security solution in terms of performance.

3.1 Proposal

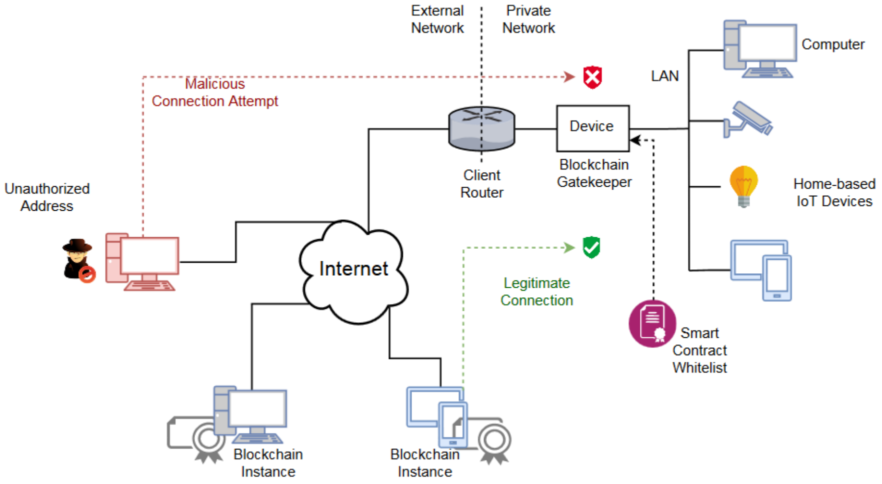


Figure 3.1. Network and logical diagram from previous work

The objective of this document was to determine the feasibility of implementing a blockchain-based network gateway. The device acts as a firewall that validates the traffic that tries to access a private home network composed of different IoT devices and personal computers. The gateway, now called the gatekeeper (GK), uses a specific smart contract with the details and rules to allow or deny access to the network. The system uses Ethereum as the underlying technology to record transactions created by the smart contract, which are parsed by a script running at the gateway that feeds a whitelist creating firewall rules that are applied and govern the gatekeeper.

3.2 Assumptions and Limitations

First, the author assumed that all blockchain entities abide by the rules of the Ethereum protocol. Second, the private Ethereum network security used for this implementation relied on its limited number of participants (nodes) and Ethereum validators (miners) that are expected to behave correctly. Only the determined nodes are assumed to have access to the Ethereum private network.

On the limitations side, the smart contracts were not secured for access or edition. The gatekeeper only provided access based on layer three information and has not been tested for any other types of attacks on the network layer. Additionally, privacy concerns have not been addressed at any level, as all transactions are public. Finally, there have not been any modifications or improvements to user experience while interacting with smart contracts. Users need to be previously exposed before operation.

3.2.1 Functionality

A private Ethereum network instance was configured on three different nodes, one of them operating at the gatekeeper. All involved computers had private Ethereum accounts that provide the interface between the users, the gatekeeper, and other components of the Ethereum blockchain. The accounts were secured by ECC, embedded in the Ethereum software suite.

The gatekeeper keeps a whitelist based on layer three information that was only modified by the smart contract and its interaction with the blockchain. The smart contract provided the authorization to the internal network, users interact with the contract through a Solidity web application, where the network information is entered, and a hash value is used for integrity. Using a Python script, the gatekeeper read all designated blockchain transactions and provided access based on information in the data field of a specific transaction. Figure 3.1 shows how the application is structured. Based on blockchain principles, all transactions can be verified by all nodes and cannot be tempered if the majority of the parties behave correctly.

3.3 Methods

The author collected data from two scenarios of the same testing environment under different conditions. During the first scenario, the network security devices ran basic whitelisting using IPTables firewall rules hosted by a Raspberri Pi device. Therefore, no blockchain interaction. During the second scenario, the devices ran all blockchain operations described previously. The data gathered was statistically analyzed to compare the two implementations.

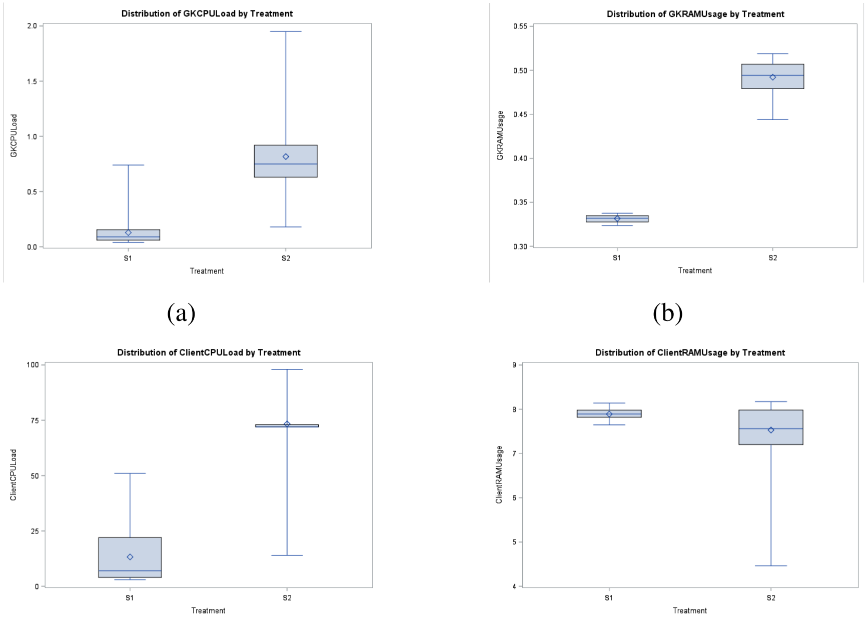
3.4 Results and Statistical Analysis

As described within the Results section of the Mendez Mena and Yang (2018) publication, the analysis of the data obtained on both experiments is determined like this:

> During both trials, 288 equally distributed samples were obtained over 24 hours for each scenario. Table 3.1 shows statistics on the data. A two-sample t-test was performed to Scenario 1 and Scenario 2 data sets to compare the performance between the two implementations with a 95% confidence level Devore (2011). The parameters used for comparison are CPU load, disk and RAM usage for the client, and gatekeeper devices. The disk usage on the gatekeeper and the client computer did not show a significant difference. The usage on both data sets did not vary, therefore, no statistical analysis was performed. Nevertheless, the CPU load ($p-value < 0.0001$), figure 3.2(a), and the RAM usage ($p-value < 0.0001$), figure 3.2(b), on the Gatekeeper, as well as and the CPU load ($p-value < 0.0001$), figure 3.2(c), and the RAM usage ($p-value < 0.0001$), figure 3.2(d), for the client computer did show statistical significance between data sets, all of them with numerical increase on scenario two, except for the client RAM usage. (p.10)

Table 3.1. *Mean and standard deviation for both testing scenarios on previous work*

Parameter	Scenario 1	σ_1	Scenario 2	σ_2
Gatekeeper CPU load [%]	0.1286	0.1038	0.8167	0.2775
Client CPU load [%]	13.2633	10.6925	73.3718	6.8044
Gatekeeper Disk Usage [GB]	1.400	0	1.400	0
Client Disk Usage [GB]	548.600	0	548.600	0.0003
Gatekeeper RAM usage [GB]	0.3316	0.0039	0.4922	0.017
Client RAM usage [GB]	7.8915	0.1109	7.5314	0.5711
# of authorized packets/sample at GK	555,493	-	3,223,788	-
# of dropped packets/sample at GK	120		248	-
# of active/passive connections/sample at GK	2.75	-	38.75	
# of connection resets/sample at GK	1.25	-	3.5	-
Time taken to add IP address to blockchain [ms]	N/A	-	49.463	-
Time taken to apply whitelisting script [ms]	N/A	-	15,322.5	-



(a) (b)

(c) (d)

Figure 3.2. Box Plot: (a) GK CPU load, (b) GK RAM usage, (c) Client CPU load, and (d) Client RAM usage.

3.5 Discussion

The author within the Discussion section (Mendez Mena & Yang, 2018) stated the following based on the information form the section above:

> The results obtained at the client computer level on the CPU load was expected since scenario two carried other tasks, such as mining and peer-to-peer communication. However, the client's disk usage did not increment significantly even though over 70,000 Ethereum blocks were processed over the sampling period. The RAM usage value on the first scenario surpassed the second one, which could be inferred that running an Ethereum node does not decrease device performance.
>
> On the Gatekeeper, the CPU load and RAM usage presented significant differences, see Table 3.1. Even though the processing capacity of the RaspberryPi is far more limited than the client computer used in the study, numerically, it cannot be considered as a burden for the device. The overall CPU usage never increased over 2%, and the RAM usage, value did not surpass the 51% mark when sampled, which

> means no memory scarcity was suffered by the embedded device and a heavier load can be applied on future applications. The disk usage, as well, did not registered a change within sampling periods, which did not go over 1.4 GB from a 32 GB limit given by the microSD card installed. Additionally, the number of packets managed by the blockchain-enabled scenario was higher than the ones from the first implementation, same with active/passive connections handled. The dropped packets and reset connections showed the same behavior. (p. 11)

3.6 Publication Conclusions

The author concluded that the use of whitelisting techniques is viable to implement using a blockchain-based scheme to protect home networks and the IoT Smart Home devices that reside in them. The blockchain capabilities provide an additional layer of protection against cyber-attacks and other actors that might try to interfere or manipulate the output of the whitelist based on faulty information. As the author described within the Conclusion section of the Mendez Mena and Yang (2018) publication:

> The cryptographic features of the Ethereum protocol, such as asymmetric key encryption and digital signatures, strengthened peer-to-peer communications between network nodes. The author considered that the results could be qualified as the starting point to a secure home-based network architecture model for IoT devices. Additionally, the distributed computing properties of the blockchain open the door for future opportunities for decentralized whitelisting based on information generated from different trusted sources. (p. 12)

3.7 Summary

In this chapter, the author summarized a previous publication on a blockchain-based security proof-of-concept aimed to provide an option to secure home-based networks and IoT devices. This publication served as the starting point for this research as it describes the viability of affordable devices with shared intelligence over a blockchain network. In the following chapter, the author introduces the security framework that leverages on previous findings to provide a holistic cybersecurity approach.

CHAPTER 4. DECENTRALIZED ACTIONABLE CYBER THREAT INTELLIGENCE FOR NETWORKS AND THE INTERNET OF THINGS

In the following chapter, the author provides a summary of his work (Mendez Mena & Yang, 2020). In this publication, the author presented a blockchain-based security framework to share actionable Cyber Threat Information (CTI) between different levels, including service providers (SP) and home networks to protect IoT devices. The author simulated a routed network that included different autonomous systems and their respective customers to recreate a practical testing environment. The numerical data obtained were subject to statistical analysis and comparison to a simple security solution in terms of performance and security functionality.

4.1 Cyber Threat Intelligence & The Blockchain

A known way to reduce the time between computer or network compromises due to cyber attacks by applying proactive protective measures is called Cyber Threat Intelligence (CTI). CTI is factual, relevant, actionable, and valuable information used by security professionals to protect their assets from cyber threats (Tounsi & Rais, 2018). Even though such information supports the efforts of the information security community, the sources of the data are reluctant to share it with external parties as it might contain sensitive information, privacy concerns, lack of trust, as well as classification and interoperability from the receiving side (Jasper, 2017). On top of it, the research published by Tounsi and Rais (2018), included quality and budgeting issues, as well as the absence of legal reliance, present themselves as a roadblock for widespread CTI sharing. The way to succeed utilizing the available information to produce effective, coordinated, and meaningful incident response actions is to collect the data from reliable sources (Wagner, Dulaunoy, Wagener, & Iklody, 2016). From the IoT perspective, to take advantage of first-hand information through a secure method, it is valid not to assume central trust as equal access, and quick propagation for action is required. Therefore, as stated by Cha, Singh, Pan, and Park (2020), the blockchain can be considered a suitable candidate for sensitive-data sharing, in this case by the implementation of a CTI system architecture for sustainable shared computing.

Over the last few years, the infosec research community has discussed the additional capabilities of blockchain technology by proposing novel applications. (Atlam, Alenezi, Alassafi, & Wills, 2018, p. 359) stated the following: “Information immutability, decentralization, anonymity (with public key protocols application), resiliency, trust, and increased computing capacity as blockchain competences that can be used to address some of the security challenges presented by the IoT.”

Ølnes, Ubacht, and Janssen (2017) expanded on the benefits and promises of the blockchain by including transparency, auditability, increased control (by consensus), data integrity, error reduction (by automation), enhanced access to information, reliability, data security, and decreasing transaction costs (by no human involvement). Hughes et al. (2019) also include automation, streamlined processes (by smart contract enforcing), and increased processing speed (due to disintermediation) where inter-organization reconciliation of data and processes could be benefited by using the blockchain, which also relates to “significant cost savings” (p. 119). Nevertheless, the same authors listed above (Atlam et al., 2018; Hughes et al., 2019; Ølnes et al., 2017) stressed the importance of acknowledging the limitations of the blockchain technology given by overall processing power, storage capabilities over time, scalability, computing costs, and privacy concerns. Consequently, the potential applicability of the blockchain also relies on design decisions and application build-out process (Ølnes et al., 2017), making clear that not all security issues of the IoT could be silver-bulleted by a blockchain application.

As new threats emerge, Cyber Threat Information (CTI) sharing becomes more important and the challenges it faces are also more apparent. Hence, the focal point for new CTI sharing applications is to understand current struggles and develop comprehensive requirements to provide valid solutions. In addition, as the threat landscape expands, it becomes even more burdensome for individual defenders to safeguard their networks by themselves. A valid pathway to achieve proactive security operations is to share dependable and trustworthy information with other parties that share the same ethic principles, something that has already been followed by many organizations (Al-Ibrahim, Mohaisen, Kamhoua, Kwiat, & Njilla, 2017). The work published by Böhm, Menges, and Pernul (2018) stated that CTI exchange is able to improve the network defense capabilities significantly as long as the information shared is “integrity-proof”(p.2). Moreover, Mtsweni and Mutemwa (2019) called for the quick and truthful exchange of relevant CTI, within the appropriate volume, between trusted partners. Nevertheless, even after realizing the benefits existing by sharing intelligence information, many organizations refrain from the exchange as they are concerned over security, privacy, and competitivity issues that have halted the initial efforts to send and receive valuable first-hand data which compromises the overall quality of the information allowed to cross-organizational borders (Al-Ibrahim et al., 2017). A truthful exchange experience requires not only sustainable quality of reports over time, but also fair and equal participation without “free-riding” by holding all actors accountable while maintaining a comfortable level of privacy and/or anonymity. The information security community also needs to consider the entire spectrum of available data, from single users to structured multinational corporations, as each one is capable of providing relevant information. However, we need to understand how each one of the participants may have different priorities when it relates to CTI. For instance, some small businesses in developing countries try to increase profits by cutting down all expenses, security included. Those owners might prefer to take the risk by not being part of CTI due to lack of proper funding (Berndt & Ophoff, 2020; V. G. Li et al., 2019). Moreover, the investment level is also reflected in the data quality within CTI notifications. Open communities share their information without structure, “such as PDF and Word documents” (Abu, Selamat, Ariffin, & Yusof, 2018) (p. 375), while Enterprise-level organizations usually include structured data to facilitate automation. It is appropriate, then, to advocate for the democratization of CTI access.

It is possible, then, to assume that the blockchain is capable of providing high availability to share data between users and service providers, as well as between ISPs. It is also safe to assume that the blockchain could maintain a distributed tamper-proof repository where CTI can be exchanged transparently, democratizing access to the data (Atzori, 2016). This blockchain platform can be assembled at the consumer level, or at the ISP level, in which the security measures can be enforced at the source or destination of the detected malicious activities. Furthermore, academic literature shows different perspectives on how to reduce the existing gaps for exchanging CTI. The work published by Cha et al. (2020) proposed a framework for sharing computational power with sustainability over time to improve efficiency. Wu, Qiao, Ye, and Lee (2019) used the blockchain to deal with trust and quality concerns as it engaged users to participate in CTI distribution. Also, Buber and Sahingoz (2020) introduced a consensus framework to safely add reports into a CTI database. The work presented by Hajizadeh, Afraz, Ruffini, and Bauschert (2020) controlled software-defined networking (SDN) systems using a distributed ledger to mitigate network threats based on activity reports shared between participants. In addition, Purohit, Calyam, Wang, Yempalla, and Varghese (2020) defended the quality of CTI reports by establishing distributed control over free riding and false reporting to effectively target threats at the cloud services level. Therefore, the published paper presented in this chapter proposes the utilization of first-hand data gathered from customers and ISPs, by their network components, such as IoT devices, and dedicated detection systems to share intelligence information distributively by using the blockchain. The main objective of this design is to address issues of current CTI sharing applications that include trust, integrity, reliability, resiliency, and unequal access to valuable information.

4.2 Materials

The author considered a simulation environment suitable ground to replicate network actors as close as possible to a real network implementation. The entire experiment was implemented using Microsoft Azure cloud services due to its virtualization nesting capabilities and other blockchain-related tools and other development applications available. The main network was simulated using the GNS3 software, Linux-based virtual machines to connect the simulated network to the outside, and Microsoft workbench applications for the web interaction with the consortium Ethereum network configured in the cloud. Figure 4.1 describes the connections of all the components used during the simulation.

Refer to Figure 4.2, as it represents the proof-of-authority Ethereum consortium that shows how the leading member is composed and how it interacts with the rest of the network. The Microsoft Azure Ethereum templates permitted rapid and scalable deployments for different organizations that want to participate in the exchange of Ethereum transactions. The deployment over the cloud also enabled performance upgrades that can be adjusted to the computing power needed within the budget capabilities of each actor. The Micorsoft Azure platform for Ethereum

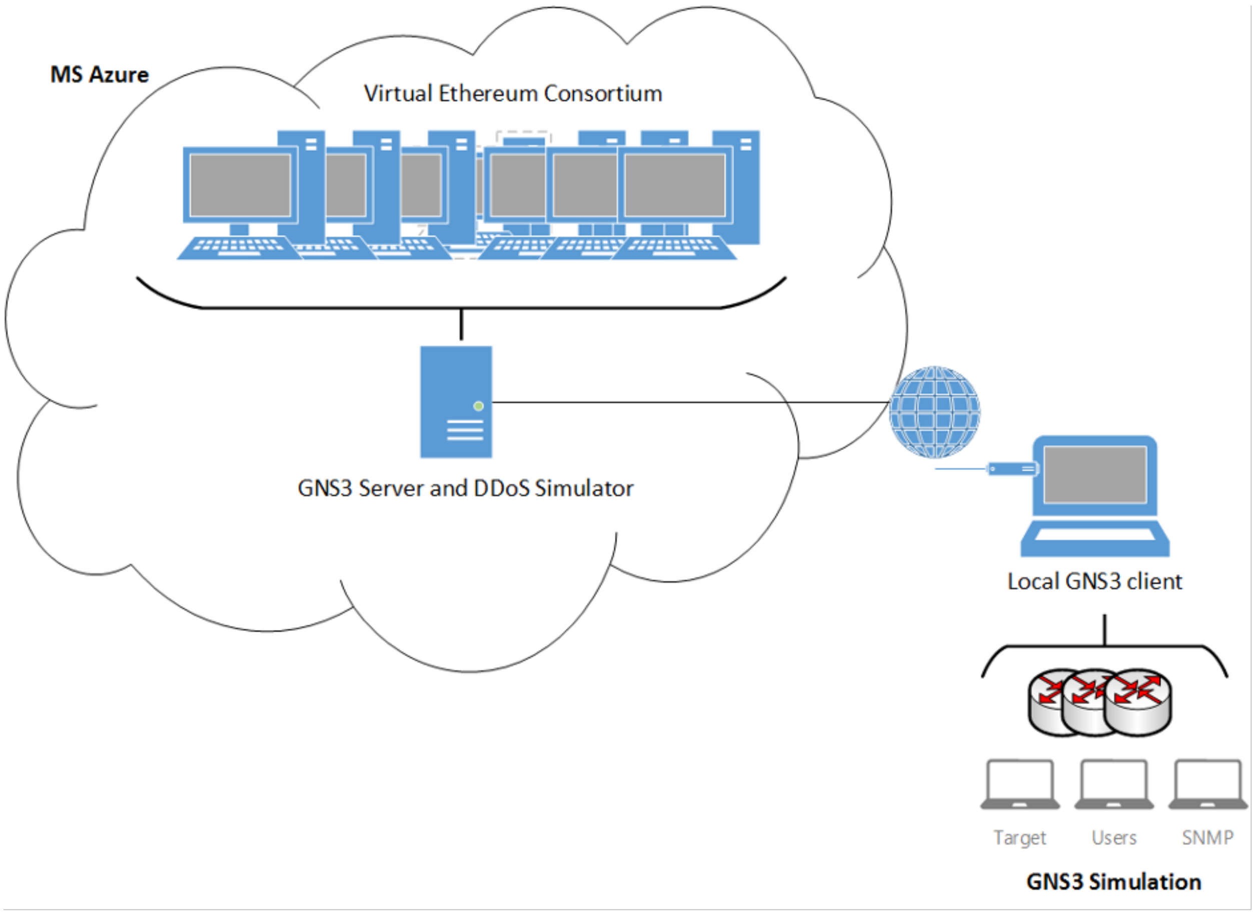


Figure 4.1. Connectivity scheme of the network simulation environment.

also allowed fair distribution of administrative rights between the consortium members, if the leader decides to distribute its initial decision power.

The Ethereum network for this deployment is governed by two smart contracts that desegregate the system in two tiers, the ISP-level tier and the user-level tier. The ISP-level tier is composed of all ISPs that have decided to participate in the CTI exchange and the user-level tier is determined by all customers that have decided to opt-in and their respective ISP. The purpose of the design is to maintain user and ISP privacy. The consumers will share data with their ISP as determined by their service agreements and the ISP will be able to share CTI between their SP-level peers without compromising user-level data. The Ethereum consortium network uses a Proof-of-Authority consensus algorithm that suits well the purpose of this application as only permissioned nodes are allowed, as well as maintaining a reasonable and efficient amount of computing power needed to validate transactions unlike Proof-of-Work schemes.

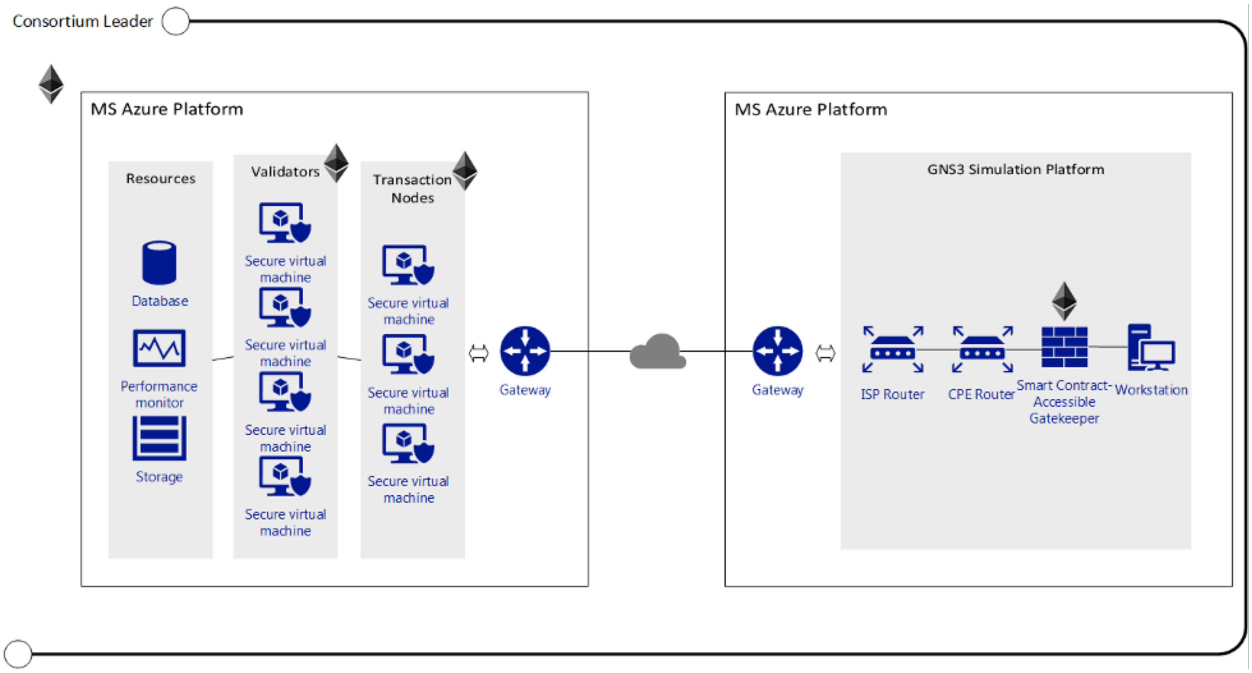


Figure 4.2. Ethereum consortium leader network scheme.

4.3 Methods

A Distributed Denial of Service (DDoS) ICMP (Internet Control Message Protocol) attack was crafted to hit a specific target inside the simulation network to test how the proposed framework work under pressure. The main objective was to demonstrate the effectiveness and efficiency of the application while stopping malicious traffic, including scanning, malware propagation, and infection, without consuming too many resources. The experiment consisted of three categories: network performance, Ethereum network performance, and network security capabilities.

To understand how the tool managed the available ISP resources, the author monitored the memory, CPU, and link usage of all the network devices that interact in data exchange. Also, the performance of the Ethereum network was evaluated to determine the effect of using the blockchain at the ISP level. Finally, the attack simulation provided the data to determine the real capabilities of the framework, as well as its limits. A statistical analysis was performed over the performance data to determine differences between network utilization with and without the blockchain. The testing scenarios used the same simulation setup, Figure 4.3 shows the GNS3 layout that was hosted at the Azure cloud. Additionally, the network performance on video streaming was also measured to determine variations at the user level when the blockchain is in place or not.

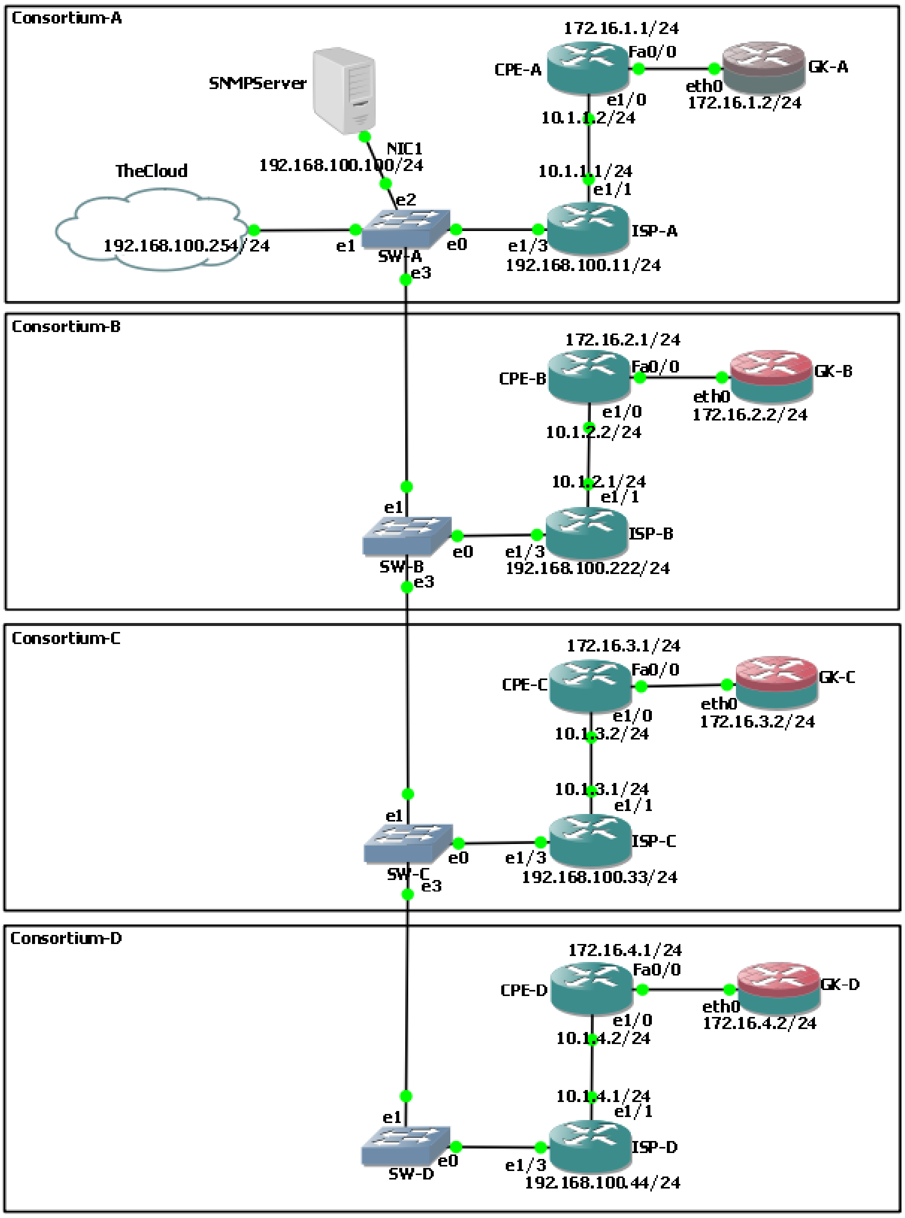


Figure 4.3. GNS3 network simulation.

Table 4.1. *Mean and standard deviation for utilized bandwidth on routers (Kbps).*

Device	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
ISP A	93,911.1	561,846	41,443.9	125,030	0.0001
ISP B	148,817	427,260	77,338.0	236,503	0.0001
ISP C	141,282	525,158	84,225.6	381,451	0.0001
ISP D	138,587	326,974	86,659.6	395,937	0.0001

4.4 Results and Statistical Analysis

The author described within the Results section of the Mendez Mena and Yang (2020) publication the following:

> The simulation ran for fourteen days in total, where the first seven were used as a "Control" group, and the other seven days, the "Experiment" group, used the blockchain to run the proposed framework. Over 66,000 equally distributed samples were collected to measure device performance, including Bandwidth (Table 4.1), CPU utilization (Table 4.2), and Response Time (Table 4.3). A random web traffic generator was used for both groups using the same seed value.
>
> Tables 4.1–4.3 show the statistics and the comparisons between the "Control" and the "Experimental" group. The p-value resulted of the two-sample t-tests performed for each group an device at the 95% confidence level. In addition, Table 4.4 presents the statistical comparison for video streaming performance again between both groups. Finally, Table 4.5 show information that belongs to the Experimental group only as only Ethereum data was available for this section of the experiment.

The tables below were taken from the same Mendez Mena and Yang (2020) publication for didactic purposes. The tables present the statistics of the collected information form all the experiments, as well as the results of the statistical comparison between the Control and Experimental group.

Figure 4.4 shows the Intrusion Detection System (IDS) alert after finding thousands of ICMP packets in a short period of time, which triggered the response on the right that include Ethereum transactions, warning the rest of the network. Figure 4.5 presents the result of the

Table 4.2. *Mean and standard deviation for CPU utilization on routers (%).*

Device	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
ISP A	7.1170	0.5006	5.9493	0.8178	0.0001
ISP B	10.0074	0.6429	8.8812	1.0412	0.0001
ISP C	9.3924	0.6639	8.3844	0.9352	0.0001
ISP D	8.9934	0.6809	8.4193	0.9244	0.0001
CPE A	0.7047	0.7238	1.4948	0.7455	0.0001
CPE B	2.1427	0.3847	2.0402	0.2254	0.0001
CPE C	2.1498	0.3972	2.0497	0.2758	0.0001
CPE D	1.1416	0.4732	1.6144	0.6150	0.0001

Table 4.3. *Mean and standard deviation for response time on routers (ms).*

Device	Control (C)	σ_1	Experimental (E)	σ_2	p-Value (H_0:$C = E$)
ISP A	6.5536	3.0634	6.5534	3.1351	0.9965
ISP B	6.4850	3.1223	6.6552	3.1151	0.0005
ISP C	6.6789	3.1686	6.7461	3.1357	0.1720
ISP D	6.6051	3.1133	6.7355	3.1440	0.0077
CPE A	18.0294	5.3292	18.3166	5.3124	0.0006
CPE B	18.1483	5.2870	18.3320	5.3395	0.0270
CPE C	18.5355	5.3244	18.5856	5.3603	0.5491
CPE D	18.4437	5.3562	18.5881	5.2901	0.2094

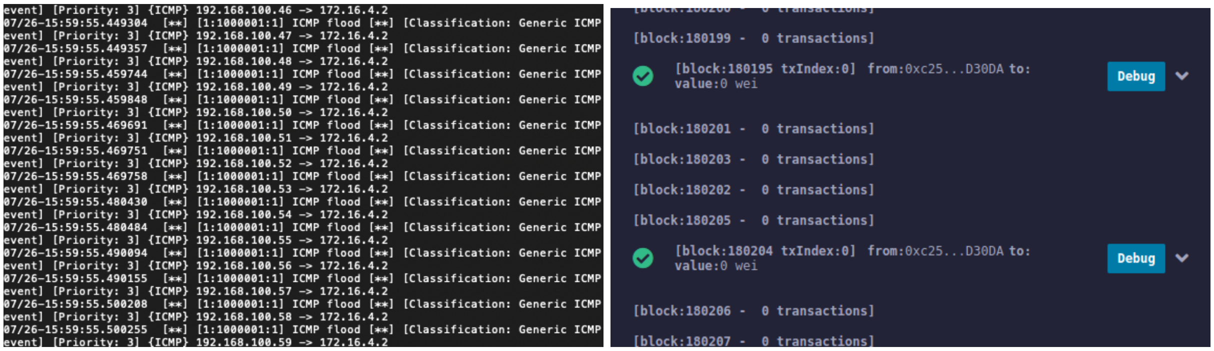
Table 4.4. *YouTube streaming performance comparison.*

Parameter	Control (C)	σ_1	Experimental (E)	σ_1	p-Value (H_0:$C = E$)
Frames Dropped	136.1	61.9451	300.6	128.3	0.0001
Resolution	640 × 360@25	-	640 × 360@25	-	N/A
Connection Speed	12,831.2 Kbps	2962.7	9827.4 Kbps	3711.5	0.0027
Buffer Health	120.9 s	6.7602	121.3 s	9.7353	0.8375

Table 4.5. *Blockchain data taken from consortium validators hosted in Microsoft Azure cloud platform.*

Parameter	Mean	$\overline{\sigma}$	Unit
Block Propagation	327.0002	96.2419	ms
Block Creation Time	4.4586	1.9444	s
Daily RPC Traffic	0.9638	0.7663	MB
Validator CPU Usage	36.9991	1.1185	%
Validator Available RAM	44.3309	3.0810	%
Validator Disk Usage	13.3417	0.3203	%

warnig triggered that initiated firewall action on the target. The graph shows on and off behavior to highlight the effect of the blockchain controls that could be in place. The security response effectively stopped the reception of malicious packets at the gateway.



```
event] [Priority: 3] {ICMP} 192.168.100.46 -> 172.16.4.2
07/26-15:59:55.449304  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.47 -> 172.16.4.2
07/26-15:59:55.449357  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.48 -> 172.16.4.2
07/26-15:59:55.459744  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.49 -> 172.16.4.2
07/26-15:59:55.459848  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.50 -> 172.16.4.2
07/26-15:59:55.469691  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.51 -> 172.16.4.2
07/26-15:59:55.469751  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.52 -> 172.16.4.2
07/26-15:59:55.469758  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.53 -> 172.16.4.2
07/26-15:59:55.480430  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.54 -> 172.16.4.2
07/26-15:59:55.480484  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.55 -> 172.16.4.2
07/26-15:59:55.490094  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.56 -> 172.16.4.2
07/26-15:59:55.490155  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.57 -> 172.16.4.2
07/26-15:59:55.500208  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.58 -> 172.16.4.2
07/26-15:59:55.500255  [**] [1:1000001:1] ICMP flood [**] [Classification: Generic ICMP
event] [Priority: 3] {ICMP} 192.168.100.59 -> 172.16.4.2
```

```
[block:180199 -  0 transactions]

✓  [block:180195 txIndex:0] from:0xc25...D30DA to:
   value:0 wei                                          Debug

[block:180201 -  0 transactions]

[block:180203 -  0 transactions]

[block:180202 -  0 transactions]

[block:180205 -  0 transactions]

✓  [block:180204 txIndex:0] from:0xc25...D30DA to:
   value:0 wei                                          Debug

[block:180206 -  0 transactions]

[block:180207 -  0 transactions]
```

Figure 4.4. (**left**) Snort security event alert. (**right**) Blockchain transactions triggered by the alert.

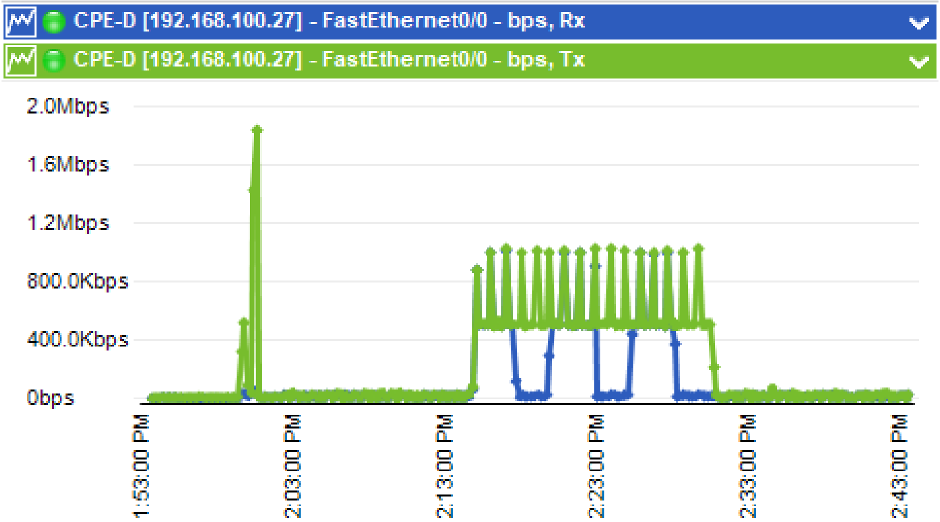


Figure 4.5. Router interface of target host, received and transmitted packets.

4.5 Discussion

Both, ISP and customer networking devices showed statistically significant differences within Bandwidth and CPU utilization. Despite the author's perceptions, the mean values for the Control group were higher than the ones obtained within the Experimental group. Further statistical analysis, the Control group data set showed a higher standard deviation, which meant that the differences between points were greater than in the Experimental setup. It is important to note that the traffic carried by the Experimental group devices included blockchain and CTI data, it also utilized other computer resources, such as IPTables and Python scripting for automated firewall rule implementation. The experiments showed that the implementation of the blockchain-based network security controls saved clock cycles and bandwidth by providing a quick response to cyberattacks at the ISP transaction level. Nevertheless, the customer premises equipment (CPE), placed at the edge of the home network did indicate higher CPU utilization as it managed higher traffic loads created by blockchain transactions. Nevertheless, the numerical results showed that the increment for all indicators is manageable and, during the analysis, the author believed the burden is outweighed by the benefits of providing additional security for ISPs and their customers. Similarly, the streaming video data indicated a slight decrease in performance within the experimental group. However, visually the changes are not distinguishable as both groups operated at 640x360 pixels with 25 frames per second rate.

From the security perspective, the blockchain data indicated that in average it took 4.4586 seconds to deliver CTI data across the network. The speed provided by the Ethereum network provided evidence that the enforcement of security controls could be expedited and spread denial of service might be controlled from the source. For instance, stopping each one of the botnet stages as listed in Figure 4.6. Moreover, the automation of the response removed the human error variable from the response equation, which increases the possibility of performing planned actions in a timely manner. In summary, the framework proposed in this work show that tamper-proof CTI data shared over a secure network that do not require trust nor a centralized entity is plausible without ignoring CTI requirements as listed by Al-Ibrahim et al. (2017); Böhm et al. (2018); and Mtsweni and Mutemwa (2019). Finally, the blockchain data did not show a resource-starving situation for Ethereum validators since the consensus algorithm used a proof-of-authority approach that eases the computational requirements compared to proof-of-work implementations. A scalable solution seems to be more appealing to service providers, that in this case, would do the heavy-lifting tasks, such as data verification and transaction dissemination. It allows actors to consider opt-in without giving up a significant investment, allowing smaller SPs to participate and benefit as much as the larger ones.

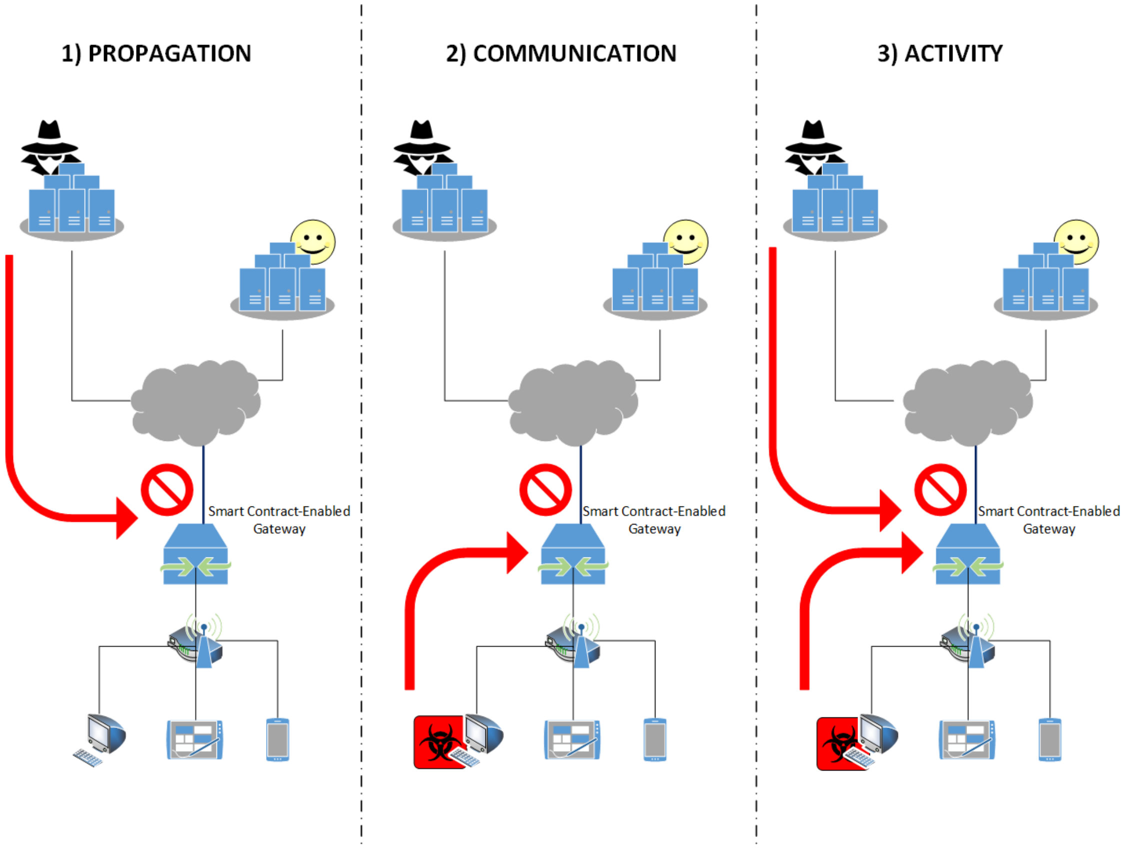

1) PROPAGATION
2) COMMUNICATION
3) ACTIVITY
Smart Contract-Enabled Gateway
Smart Contract-Enabled Gateway
Smart Contract-Enabled Gateway

Figure 4.6. Cyber threat intelligence (CTI) enforcing diagram during three stages of a botnet attack.

4.6 Conclusions

The author showed the viability of implementing a decentralized CTI sharing network that involved service providers and customers. The data indicated that first-hand information disseminated throughout a secure and tamper-proof intelligence data is capable of alleviating the effect of a massive denial of service attack due to rapid incident response with no initial human intervention. Even though it existed a statistically significant difference in terms of traffic load and computing resources within the Experimental group, it did not relate to a user experience degradation. The results indicated that this framework could be viewed as the starting point for additional protection based on CTI information where access is democratized.

4.7 Summary

In this chapter, the author summarized previous work on a CTI sharing network over a decentralized Ethereum network aimed to provide an option to secure home-based networks and IoT devices and ISP networks.

CHAPTER 5. FUTURE WORK, SUMMARY, CONCLUSIONS, & RECOMMENDATIONS

In the following chapter, the author summarizes the future proposal for publication work authored by the writer of this document. In this section, the author presents a blockchain-based security framework to share actionable Cyber Threat Information (CTI). The proposal includes different levels including service providers (SP), and home networks to protect IoT devices. The notifications offered are machine-actionable, which includes privacy protections. The author proposes a theoretical framework that utilizes standardized structured reports within different privacy levels to stimulate collaborations between organizations, and users. The following approach, differing from previous publications, introduces the implementation of CTI notification standards, allowing interoperability with other cyber intelligence sharing platforms. Standardization with structured text allows the escalation with other security tools, reaching even more networks and devices than previously intended. Moreover, the new framework adds privacy controls to enable users and providers to manage, using the introduced standard properties and other protocols, how their information is seen, and shared. Also, it utilizes novel software-based network controls to warrant additional network corrective measures during cyber attacks. In a nutshell, the author presents a decentralized machine-actionable framework for standard CTI distribution to secure the IoT and home networks.

5.1 CTI Standards, Privacy Solutions, & the Blockchain

Cyber Threat Intelligence information cannot be considered valuable if it is not shared with corresponding parties. However, as stated previously, it exists some privacy concerns between different organizations and users that prevent full collaboration. An additional challenge CTI info sharing faces is data quality. Modi (2020) lays out some basic requirements for CTI reports that include the need to be operational as well as actionable. To comply with the formerly mentioned requirements, it is essential that the data to be shared is normalized and machine readable. In other words, it needs to be standardized, so other parties can obtain the value they hope. Standardized, and measurable CTI data are the most important efforts made by the InfoSec community to improve collaboration (Ramsdale, Shiaeles, & Kolokotronis, 2020). In fact, the US Department of Homeland Security (DHS) formerly, and now the Organization for Advancement of Structured Information Standards (OASIS) have led the initiatives to delineate CTI data sharing. Such strategy has paved the way for the inclusion of the standards called structured threat information expression (STIX) (OASIS, 2017), trusted automated exchange of indicator information (TAXII) (OASIS, n.d.-b), and cyber observable expression (CybOX) (OASIS, n.d.-a). Those protocols and guidelines have become the norm for structured CTI within the community. Nevertheless, according to Fisk et al. (2015), unstructured or informal sharing is still the most common between organizations.

Other challenges for CTI sharing include chances for exploitation of the public information, the reputation that could be affected by identifying the source of the traffic, and public vulnerabilities under attack (Badsha, Vakilinia, & Sengupta, 2019). Fisk et al. (2015) defined three primary principles for CTI data sharing as well as engineering principles to develop sharing applications. The list includes least disclosure, qualitative evaluation (technical and legal), and forward progress (not being paralyzed by the previous two). Such principles make sense since the real legal implications organizations need to review thoroughly, as different regions present their own regulations. Data sharing in the US might not be allowed in the same way in Europe, so all parties involved need to be comfortable with all policies and obligations for sharing (Sullivan & Burger, 2017).

The Information Security CTI literature shows different articles that propose solutions to the problems described above. The solutions come from academia as well as from industry organizations. For instance, a private conglomerate of incident response teams formed a different type of decentral communities (based on market vertical) called “Information Sharing and Analysis Centre” (ISAC) (ENISA, 2019). ISACs are the focal point for CTI data exchange where different sides share their experiences and notifications of ongoing cyber-attacks. Their privacy protections abide by the Traffic Light Protocol (TLP) (FIRST, 2019), which tell the community what and whom to distribute. The academia has also come up with technical ways to protect privacy while sharing sensitive information. Sadique, Cheung, Vakilinia, Badsha, and Sengupta (2018) proposed the inclusion of sensitivity levels to safeguard the confidential information. Their initiative includes four different approaches, that go from open text to encrypted subscription-only Private Set Intersection (PSI).

The work published by Hajizadeh et al. (2020) brought up the importance of response time during a cyber crisis. Verizon (2015) showed that target realignment takes less than 24 hours 70% of the time for the first two targets, and less than an hour to reach the third one. Mcmahon, Canada, and Howes (2013) also stressed the importance of a quick response to incidents with Near Real Time (NRT) CTI to develop a proactive defense of network infrastructure. Hajizadeh et al. (2020) proposed a CTI data sharing solution that leverages in the properties and benefits that the blockchain offers. The architecture proposed combines such advantages with current network management technological tendencies, such as Software Defined Networking (SDN), to automate a response to DDoS attacks.

In fact, Software Defined Networking, which removes the dependency between the data and control plane within network devices, has become some of the most important tools when researchers try to find the way to respond as quickly as possible from the service provider side. Wani et al. (2021) reviewed the latest development of DDoS mitigation techniques using the blockchain and SDN technologies (Abou El Houda, Hafid, & Khoukhi, 2019b, 2019a; Ahmed, Danish, Qureshi, & Lestas, 2019; Rodrigues, Bocek, Lareida, et al., 2017; Rodrigues, Bocek, & Stiller, 2017). Researchers used a Blockchain-only (Al-Sakran, Alharbi, & Serguievskaia, 2019; Giri, Jaisinghani, Kriplani, Ramrakhyani, & Bhatia, 2019; Misra, Deb, Pathak, & Mukherjee, 2020), artificial intelligence detection methods (Manikumar & Maheswari, 2020; Mtsweni & Mutemwa, 2019), collaborative-only (Rodrigues, Scheid, Killer, Franco, & Stiller, 2020), and hybrid (Al-Sakran et al., 2019) approaches to deal directly against distributed denial of services attacks using smart contracts and SDN.

5.2 Framework Proposal

The following proposal is based on previous work published and described in sections above (Mendez Mena & Yang, 2018, 2020). The purpose is to add privacy, hollistic enforcement, and automation enhancements to the architecture that has been already tested in terms of efficiency and security. The objective is to offer near real time (NRT) containment based on first-hand CTI data that can be actioned locally, at the user, or the service provider level by leveraging from the properties of a consortium Ethereum blockchain network.

5.2.1 Architecture Description

The system uses first-hand traffic information that triggers a response based on open-source IDS software installed at the edge of the home network. The enforcement equipment will automatically deploy firewall rules based on local or network CTI information that has gone through a validation process controlled by the service provider. To comply with the validation process running within the blockchain consensus algorithms, the system will keep the two-layer design, as in Mendez Mena and Yang (2020). The two-level approach helps maintaining basic privacy over the data shared as the users will only share CTI data between their service provider and its customer network, which is ruled by their legally-binding private service contracts. On the other hand, the collaboration between service providers needs to be sustained by privacy protections. Privacy safeguards need to be taken when the data is obtained and validated with their own CTI information before being shared with other providers in the network. Both levels are governed by two Ethereum smart contracts that delineate the rules for interaction and segregate levels. The smart contract created for the user layer allows exclusive sharing between individual users and their ISP. The user layer contract protects any type of customers' personal information from being shared with third parties beyond what has been legally stated within their service contracts. The smart contract used to delimit the ISP layer allows data validation, error correction, and distribution of the aggregated or redacted data collected at the user level. The ISP contract also determines the responsive or preventive actions to be taken whenever a cyber threat has been detected throughout the Ethereum network.

The underlying blockchain network can provide a decentralized, tamper-proof, immutable, auditable platform that offers easy access while offering data integrity over a trustless network (Hughes et al., 2019; Ølnes et al., 2017). Previous work from the author provides evidence on the efficiency capabilities offered by the blockchain for home network gateways and for ISP-owned nodes. It also shows how the system behaves under cyber attacks that trigger IDS signatures and, therefore, the automated blockchain transactions that share the notifications with the rest of the system. The NRT rapid dissemination of verified and integrity-proof CTI information of quality can significantly improve defense capabilities of cybersecurity systems and teams (Mtsweni & Mutemwa, 2019).

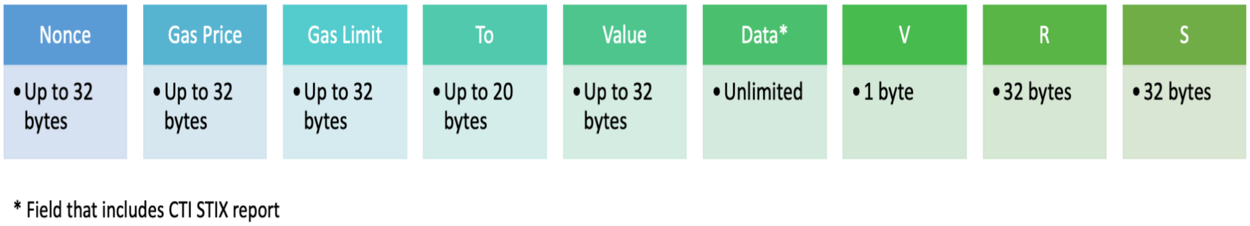
One of the additions to previous frameworks proposed by the author, it is the inclusion of structured language for CTI notifications into the Ethereum block data field. Many CTI communities still use informal notices for ongoing threats (Fisk et al., 2015), making the information human-only readable, un-actionable, and therefore, un-operational. The United States Department of Homeland Security (DHS) launched the initiative to standardize cyber intelligence information, and came up with the Structured Threat Information eXpression (STIX) format (OASIS, 2017). The now standard, based on the JSON language, provides a way to make CTI information machine ready, so it can be applied automatically. Listing 5.1 shows a STIX notification example for a report on a single IPv4 address. Listing 5.2 shows a report of an entire CIDR block that could be included in the data field of the Ethereum Block that is part of the notification. Figure 5.1 shows the Ethereum block structure that includes block number information, timestamp, difficulty information, parent hash, state, and also incorporates a data field. The data field will be used to carry STIX-formated notifications received from the detection tool installed at the customer network edge, such as described in Listings 5.1 and 5.2.

```
{
  "type": "ipv4-addr",
  "spec_version": "2.1",
  "id": "ipv4-addr--ff26c558-8523-5tc8-r88t-69f8963214ee",
  "created": "2021-03-28T19:37:11.213Z",
  "modified": "2021-03-28T19:37:11.213Z",
  "first_observed": "2021-03-27T21:37:11.213Z",
  "last_observed": "2021-03-27T21:37:11.213Z",
  "number_observed": 1,
  "value": "221.32.192.8"
}
```

Listing 5.1: STIX report for IPv4 addresses (OASIS, 2017)

```
{
  "type": "ipv4-addr",
  "spec_version": "2.1",
  "id": "ipv4-addr--9658t6a8-548e-5b9s-7b5e-hth356yt6998",
  "created": "2021-03-28T19:37:11.213Z",
  "modified": "2021-03-28T19:37:11.213Z",
  "first_observed": "2021-03-27T21:37:11.213Z",
  "last_observed": "2021-03-27T21:37:11.213Z",
  "number_observed": 1,
  "value": "221.32.192.0/24"
}
```

Listing 5.2: STIX report for IPv4 CIDR blocks (OASIS, 2017)



Nonce	Gas Price	Gas Limit	To	Value	Data*	V	R	S
• Up to 32 bytes	• Up to 32 bytes	• Up to 32 bytes	• Up to 20 bytes	• Up to 32 bytes	• Unlimited	• 1 byte	• 32 bytes	• 32 bytes

* Field that includes CTI STIX report

Figure 5.1. Ethereum Block Structure

Also, the current proposal includes automated response at the network plane besides the firewall/IDS rules implemented at the blockchain-enabled gatekeeper. The self-operating response to network-based attacks, i.e. Distributed Denial of Service (DDoS) attacks, should help the rapid distribution of CTI information between service providers. Since the current framework proposal is based on a distributed scheme, the author presents an also distributed Software-Defined Networking (SDN) interaction through an open-source Application Programming Interface (API). Current distributed applications, such as ONIX (Koponen et al., 2019), ONOS (Berde et al., 2014), or SDX (Gupta et al., 2014), will be included. Their application beenfits and constraints were also reviewed by Bannour, Souihi, and Mellouk (2018). Figure 5.2 shows how the network implementation is laid out at a high level. The figure shows the two levels the framework utilizes, the Tier-One limit resides at the edge of the customer network. In this representation, we would have four different instances, each one manage by their own contract. Tier two "jurisdiction" belong to service providers, where CTI information is exchanged and actioned. The Validators (known as miners under a Proof-of-Work scheme) and the SDN controllers will serve both tiers, they will validate transactions and control routing rules respectively.

Privacy concerns are one of the main causes for which organizations are reluctant to share CTI data with other organizations. CTI reports shared with other parties might contain sensitive information, competitors may obtain inside information, reputation could be affected, attackers would get to know vulnerabilities, or simply they do not trust outside parties (Badsha et al., 2019). Organizations, and end-users need to consider the risk involved in how the data is going to be shared, governed, protected, and stored (Fisk et al., 2015). Therefore, technical privacy protections come along with policy. It is the application developer's duty to include as many privacy options as possible for each user/organization to be able to match their policy with the technical solution. The current proposal includes privacy safeguards not available during previous

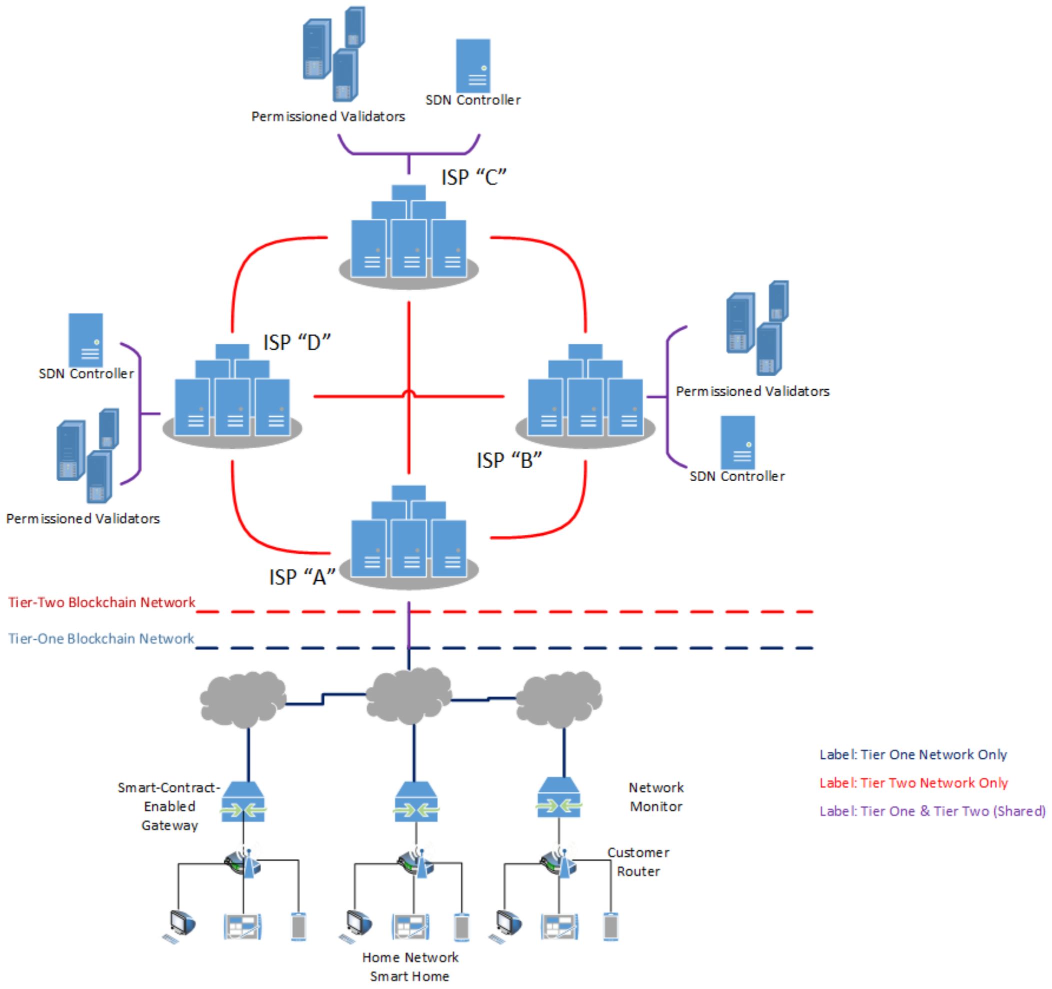


Figure 5.2. Network configuration for the proposed framework

implementations that run on top of the ones offered by the blockchain, such as pseudo-anonymity. STIX (OASIS, 2017) gives users the possibility to redact any type of information they feel could compromise their privacy. In addition, this framework proposes the inclusion, similar to ISACs communities, of the Traffic Light Protocol (TLP) (FIRST, 2019), which determines the audience and the boundaries of the information to be shared. Also, the author proposes the inclusion of expiration terms for indicators of compromise (IOC) or CTI reports. The reasoning resides on the argument that much of the information exchanged is assigned dynamically or change from target to target, such as IP addresses, URLs, or phishing campaigns. The time, initially, to keep records valid is set for 14 days, as the 0.11% of attacks may persist for this long (Cook, 2021). Finally, as notification errors are possible due to false positives or authorized actions, the author will use

STIX capabilities to manage confidence values. Those values, managed from the service provider level, could be set to zero to retire the notification should an error occur. These capabilities can be scripted at the smart contracts and the notification Python program that puts together the notifications from the IDS and the blockchain network.

5.2.2 Methodology

The author proposes two different approaches to obtain data on the tool security performance, which includes CTI spread speed and behavior under attacks. The first one is based on previous work, which utilizes simulation techniques using the Microsoft Azure Cloud Computing platform and the GNS3 network simulator. Figure 5.3 shows the simulation architecture to be used for testing during the first phase of data collection. The figure shows how the simulation platform will be set up, inclusing the GNS3 network simulator interfacing with the rest of the Ethereum workbench sitting in the MS Azure cloud. The data collected through the first experiment should provide information on how fast the system reacts to attacks as well as the time needed to reach all blockchain nodes. The experiment should also provide insights on computing resources needed to maintain a similar operation under real-world circumstances. The initial data gathering will consist of two phases, from now on called “Control” and “Experimental” groups. The Control group will not use any of the blockchain network structures. Meanwhile, the Experimental group will be run within a fully operational Ethereum consortium blockchain network. The data will be statistically compared using a two-sample t-test to determine significant differences between both groups (Devore, 2011).

The second phase of the data collection is two-folded. The first one will collect simulation data, similar to previous experiments from the author (Mendez Mena & Yang, 2020). The collection will focus on network behavior parameters gathered at the edge of the target network to determine how the system reacts to a Distributed Denial of Service attack. Figure 5.4 shows a visual representation of a use case for the Mirai botnet within the framework proposed. The representation describes Mirai’s botnet propagation, and activity stages. The first one scans for vulnerable IoT devices over port TCP 23 and 2323, and the second one is launching a SYN flood

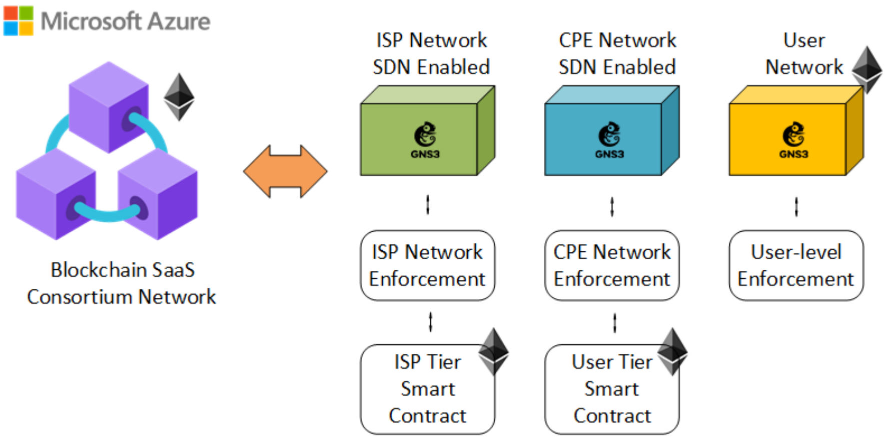


Figure 5.3. Ethereum simulation architecture

attack as part of a DDoS activity. In both cases, the blockchain-enabled application should detect, alert, and stop the activity.

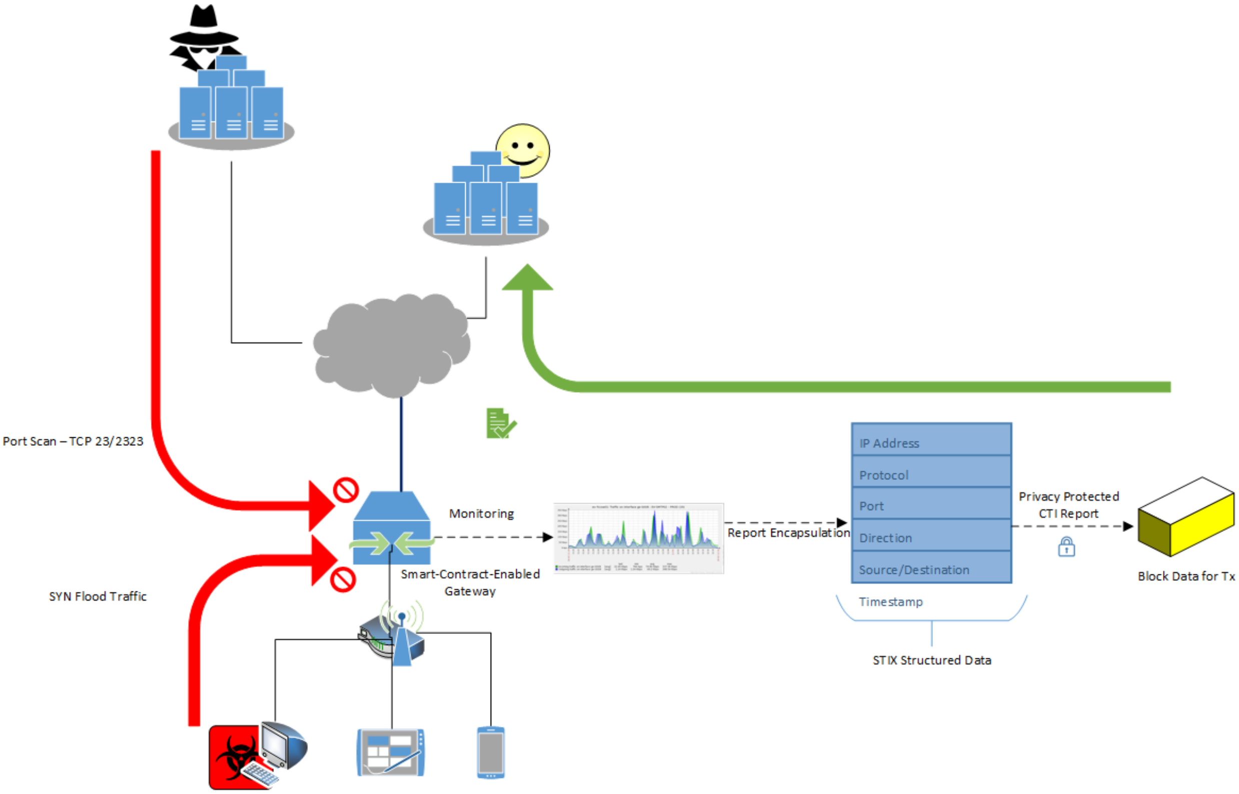


Figure 5.4. Network configuration for the proposed data collection method

The second piece will utilize an external DDoS botnet attack on IoT devices data set, such as the one collected and published by Siddharth (2020). The objective is to recreate a different type of attack that includes real-world data to provide an integral inference of the framework's security properties. Some adjustments will need to be made to the previously used network architecture to fit the environment where the external data was collected.

5.3 Proposal Summary and Conclusion

The author has laid out an enhanced proposal to protect home network and the IoT devices including the utilization of CTI standards and privacy protections. The framework aims to reduce the incident response speed by making CTI data machine readable and capable of being deployed at network security devices throughout the entire network of organizations that have decided to collaborate. The use of standards will allow the deployment of protective measures without restructuring the current network capabilities.

After collecting the indicated data and performing the respective analysis, the author plans to submit the proposed enhancements to an Information Security journal.

5.4 Overall Summary, Conclusions, and Recommendations

In this work, a machine readable and standardized cyber threat intelligence sharing and operational framework has been proposed. Throughout a series of experiments, the author has provided evidence on the efficiency and security capabilities of using the blockchain as an underlying technology used for collaboration and data exchange with the objective to secure home networks and the IoT devices that are now commonly found in them. The framework has been designed to work at the user and service provider level to deliver a holistic solution that includes all internet participants by providing fair access to a democratized intelligence information.

The results shown in this work, provide the initial attestation that an integrity-proof collaboration network for security purposes is plausible. Even though the blockchain-enabled devices did show increased requirements in terms of computer power and memory, in practice none of the devices experienced resource exhaustion nor the user experience was affected.

Moreover, the security performance of the first two publications exhibit promising results by containing cyber attacks as well as spreading notifications that allow other parties to take preventive measures in a timely manner. Therefore, the author can conclude that a distributed securing system to protect and to provoke an early response to network attacks targeting IoT devices is technologically viable.

The results of the study had limitations in terms of the number of nodes and interactive devices, as well as minimizing exclusive attacks to the blockchain and its consensus algorithms. It is recommended, then, that broader experiments that utilize real-world networks to produce more conclusive results and possible real-life or commercial applications. Finally, those future studies should include a thorough assessment of the underlying technologies and protocols to deliver safe and sound implementations able to truly deliver on their commitments.

REFERENCES

Abou El Houda, Z., Hafid, A., & Khoukhi, L. (2019b, 12). Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN. In *2019 ieee global communications conference, globecom 2019 - proceedings.* Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/GLOBECOM38437.2019.9013542

Abou El Houda, Z., Hafid, A. S., & Khoukhi, L. (2019a). Cochain-SC: An Intra-and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract. *IEEE Access*, *7*, 98893–98907. doi: 10.1109/ACCESS.2019.2930715

Abu, S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence-Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379. doi: 10.11591/ijeecs.v10.i1.pp371-379

Ahmed, Z., Danish, S. M., Qureshi, H. K., & Lestas, M. (2019, 9). Protecting IoTs from mirai botnet attacks using blockchains. In *Ieee international workshop on computer aided modeling and design of communication links and networks, camad* (Vol. 2019-Septe). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/CAMAD.2019.8858484

Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., & Njilla, L. (2017, 2). Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence. *arXiv*. Retrieved from `http://arxiv.org/abs/1702.00552`

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., ... Zanichelli, F. (2018, 4). IoTChain: A blockchain security architecture for the Internet of Things. In *2018 ieee wireless communications and networking conference (wcnc)* (pp. 1–6). IEEE. Retrieved from `https://ieeexplore.ieee.org/document/8377385/` doi: 10.1109/WCNC.2018.8377385

Al-Sakran, H., Alharbi, Y., & Serguievskaia, I. (2019, 10). Framework architecture for securing iot using blockchain, smart contract and software defined network technologies. In *2019 2nd international conference on new trends in computing sciences, ictcs 2019 - proceedings.* Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ICTCS.2019.8923080

Aman, M. N., Sikdar, B., Chua, K. C., & Ali, A. (2018, 8). Low Power Data Integrity in IoT Systems. *IEEE Internet of Things Journal*, *5*(4), 3102–3113. Retrieved from `https://ieeexplore.ieee.org/document/8354891/` doi: 10.1109/JIOT.2018.2833206

Amin, R., Kumar, N., Biswas, G., Iqbal, R., & Chang, V. (2018, 1). A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. *Future Generation Computer Systems*, *78*, 1005–1019. Retrieved from `https://www-sciencedirect-com.ezproxy.lib.purdue.edu/science/article/pii/S0167739X1630824X` doi: 10.1016/J.FUTURE.2016.12.028

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: benefits, challenges, and future directions . *Intelligent Systems and Applications*, *6*, 40–48. Retrieved from `http://www.mecs-press.org/` doi: 10.5815/ijisa.2018.06.05

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 10204 LNCS, pp. 164–186). Springer, Berlin, Heidelberg. Retrieved from `http://link.springer.com/10.1007/978-3-662-54455-6_8` doi: 10.1007/978-3-662-54455-6{_}8

Atzori, M. (2016, 1). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? *SSRN Electronic Journal*. Retrieved from `https://papers.ssrn.com/abstract=2709713` doi: 10.2139/ssrn.2709713

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In *Wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (wireless vitae), 2011 2nd international conference on* (pp. 1–5).

Badsha, S., Vakilinia, I., & Sengupta, S. (2019, 3). Privacy preserving cyber threat information sharing and learning for cyber defense. In *2019 ieee 9th annual computing and communication workshop and conference, ccwc 2019* (pp. 708–714). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/CCWC.2019.8666477

Bannour, F., Souihi, S., & Mellouk, A. (2018, 1). Distributed SDN Control: Survey, Taxonomy, and Challenges. *IEEE Communications Surveys and Tutorials*, *20*(1), 333–354. doi: 10.1109/COMST.2017.2782482

Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns. In *International conference on financial cryptography and data security* (pp. 494–509). Springer. Retrieved from `https://link.springer.com/chapter/10.1007/978-3-319-70278-0_31http://arxiv.org/abs/1703.06322%0Ahttp://dx.doi.org/10.1007/978-3-319-70278-0` doi: 10.1007/978-3-319-70278-0

Berde, P., Gerola, M., Hart, J., Higuchi, Y., Kobayashi, M., Koide, T., … Parulkar, G. (2014, 8). ONOS: Towards an open, distributed SDN OS. In *Hotsdn 2014 - proceedings of the acm sigcomm 2014 workshop on hot topics in software defined networking* (pp. 1–6). New York, NY, USA: Association for Computing Machinery. Retrieved from `https://dl.acm.org/doi/10.1145/2620728.2620744` doi: 10.1145/2620728.2620744

Berndt, A., & Ophoff, J. (2020, 9). Exploring the Value of a Cyber Threat Intelligence Function in an Organization. In *Ifip advances in information and communication technology* (Vol. 579 IFIP, pp. 96–109). Springer Science and Business Media Deutschland GmbH. Retrieved from `https://doi.org/10.1007/978-3-030-59291-2_7` doi: 10.1007/978-3-030-59291-2{_}7

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, *50*(2), 76–79.

Bhattasali, T., Chaki, R., & Chaki, N. (2013, 12). Secure and trusted cloud of things. In *2013 annual ieee india conference (indicon)* (pp. 1–6). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/6725878/` doi: 10.1109/INDCON.2013.6725878

Bohli, J.-M., Skarmeta, A., Victoria Moreno, M., Garcia, D., & Langendorfer, P. (2015, 4). SMARTIE project: Secure IoT data management for smart cities. In *2015 international conference on recent advances in internet of things (riot)* (pp. 1–6). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7104906/` doi: 10.1109/RIOT.2015.7104906

Böhm, F., Menges, F., & Pernul, G. (2018, 12). Graph-based visual analytics for cyber threat intelligence. *Cybersecurity*, *1*(1), 1–19. Retrieved from `https://link-springer-com.ezproxy.lib.purdue.edu/articles/10.1186/s42400-018-0017-4https://link-springer-com.ezproxy.lib.purdue.edu/article/10.1186/s42400-018-0017-4` doi: 10.1186/s42400-018-0017-4

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1–31.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017, 4). Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain. In *2017 ieee european symposium on security and privacy workshops (euros&pw)* (pp. 50–58). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7966970/` doi: 10.1109/EuroSPW.2017.50

Brachmann, M., Garcia-morchon, O., & Kirsche, M. (2011). Security for practical coap applications: Issues and solution approaches. *2011 10th GI/ITG KuVS Fachgespraech Sensornetze (FGSN 2011)*(Fgsn), 1–4. Retrieved from `https://www.researchgate.net/publication/265973615https://www-rnks.informatik.tu-cottbus.de/content/unrestricted/staff/mk/Publications/FGSN_2011-Brachmann_Morchon_Kirsche.pdf` doi: 10.1016/j.prevetmed.2014.12.009

Buber, E., & Sahingoz, O. K. (2020). Blockchain Based Information Sharing Mechanism for Cyber Threat Intelligence. *Balkan Journal of Electrical and Computer Engineering*, *8*(3), 242–253. Retrieved from `http://dergipark.gov.tr/bajece` doi: 10.17694/bajece.644948

Buchmann, N., Rathgeb, C., Baier, H., Busch, C., & Margraf, M. (2017, 7). Enhancing Breeder Document Long-Term Security Using Blockchain Technology. In *2017 ieee 41st annual computer software and applications conference (compsac)* (pp. 744–748). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/8030023/` doi: 10.1109/COMPSAC.2017.119

Buterin, V. (2015). *On Public and Private Blockchains.* Retrieved from `https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/`

Buterin, V. (2018, 5). Comparative analysis of blockchain consensus algorithms. In *2018 41st international convention on information and communication technology, electronics and microelectronics (mipro)* (pp. 1545–1550). IEEE. Retrieved from `https://ieeexplore.ieee.org/document/8400278/` doi: 10.23919/MIPRO.2018.8400278

Cha, J., Singh, S. K., Pan, Y., & Park, J. H. (2020, 8). Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. *Sustainability*, *12*(16), 6401. Retrieved from `https://www.mdpi.com/2071-1050/12/16/6401` doi: 10.3390/su12166401

Chen, Y., Trappe, W., & Martin, R. P. (2007, 6). Detecting and Localizing Wireless Spoofing Attacks. In *2007 4th annual ieee communications society conference on sensor, mesh and ad hoc communications and networks* (pp. 193–202). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/4292831/` doi: 10.1109/SAHCN.2007.4292831

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303.

Collen, A., Nijdam, N. A., Augusto-Gonzalez, J., Katsikas, S. K., Giannoutakis, K. M., Spathoulas, G., . . . Dimas, M. (2018, 2). GHOST - Safe-guarding home IoT environments with personalised real-time risk control. In *Communications in computer and information science* (Vol. 821, pp. 68–78). Springer, Cham. Retrieved from http://link.springer.com/10.1007/978-3-319-95189-8_7 doi: 10.1007/978-3-319-95189-8{_}7

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016, 11). Blockchain for the Internet of Things: A systematic literature review. In *2016 ieee/acs 13th international conference of computer systems and applications (aiccsa)* (pp. 1–6). IEEE. Retrieved from http://ieeexplore.ieee.org/document/7945805/ doi: 10.1109/AICCSA.2016.7945805

Cook, S. (2021). *DDoS attack statistics and facts for 2018-2021.* Retrieved from https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

Costin, A., Zaddach, J., Francillon, A., Balzarotti, D., & Antipolis, S. (2014). A Large-Scale Analysis of the Security of Embedded Firmwares. In *Usenix security symposium* (pp. 95–110).

Crosby, M., Pattanayak, P., & Verma, S. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*(2). Retrieved from https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf doi: 10.1515/9783110488951

Cruz, M. G., Peters, G. W., & Shevchenko, P. V. (2015). Fundamental Aspects of Operational Risk and Insurance Analytics: A Handbook of Operational Risk. In *Fundamental aspects of operational risk and insurance analytics: A handbook of operational risk* (pp. 1–917). Retrieved from https://www.computer.org/csdl/proceedings/sp/2016/0824/00/0824a839-abs.html doi: 10.1002/9781118573013

Cui, A., & Stolfo, S. J. (2010). A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan. In *Proceedings of the 26th annual computer security applications conference* (pp. 97–106).

Das, R., & Das, I. (2016, 9). Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques. In *2016 second international conference on research in computational intelligence and communication networks (icrcicn)* (pp. 296–301). IEEE. Retrieved from http://ieeexplore.ieee.org/document/7813674/ doi: 10.1109/ICRCICN.2016.7813674

Demirbas, M., & Youngwhan Song, Y. (2006). An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. In *2006 international symposium on a world of wireless, mobile and multimedia networks(wowmom'06)* (pp. 564–570). IEEE. Retrieved from http://ieeexplore.ieee.org/document/1648515/ doi: 10.1109/WOWMOM.2006.27

Devore, J. L. (2011). *Probability and Statistics for Engineering and the Sciences*. Cengage learning.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. In *Proceedings of the second international conference on internet-of-things design and implementation - iotdi '17* (pp. 173–178). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?doid=3054977.3055003 doi: 10.1145/3054977.3055003

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, 3). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 ieee international conference on pervasive computing and communications workshops (percom workshops)* (pp. 618–623). IEEE. Retrieved from http://ieeexplore.ieee.org/document/7917634/ doi: 10.1109/PERCOMW.2017.7917634

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017, 12). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, *55*(12), 119–125. Retrieved from http://ieeexplore.ieee.org/document/8198814/ doi: 10.1109/MCOM.2017.1700879

Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F., & Vassilacopoulos, G. (2012, 11). Enabling data protection through PKI encryption in IoT m-Health devices. In *2012 ieee 12th international conference on bioinformatics & bioengineering (bibe)* (pp. 25–29). IEEE. Retrieved from http://ieeexplore.ieee.org/document/6399701/ doi: 10.1109/BIBE.2012.6399701

ENISA. (2019). *Secure Group Communications for Incident Response and Operational Communities* (Tech. Rep. No. July). Retrieved from https://www.enisa.europa.eu/publications/secure-group-communications

Eyal, I., & Sirer, E. G. (2018, 6). Majority is not enough. *Communications of the ACM*, *61*(7), 95–102. Retrieved from http://dl.acm.org/citation.cfm?doid=3234519.3212998 doi: 10.1145/3212998

FIRST. (2019). *Traffic Light Protocol (TLP) Definitions and Usage* (Tech. Rep.). Forum of Incident Response and Security Teams. Retrieved from https://www.cisa.gov/tlp

Fisk, G., Ardi, C., Pickett, N., Heidemann, J., Fisk, M., & Papadopoulos, C. (2015, 7). Privacy principles for sharing cyber security data. In *Proceedings - 2015 ieee security and privacy workshops, spw 2015* (pp. 193–197). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/SPW.2015.23

Forbes. (2016). *152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things.* Retrieved from http://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/34bf983369a7

Gartner. (2017). *Gartner Says 8.4 Billion Connected Things Will Be in Use in 2017, Up 31 Percent From 2016.* Retrieved from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Giri, N., Jaisinghani, R., Kriplani, R., Ramrakhyani, T., & Bhatia, V. (2019). Distributed Denial of Service(DDoS) Mitigation in Software Defined Network using Blockchain. In *Proceedings of the 3rd international conference on i-smac iot in social, mobile, analytics and cloud, i-smac 2019* (pp. 673–678). Retrieved from https://ieeexplore.ieee.org/abstract/document/9032690/ doi: 10.1109/I-SMAC47947.2019.9032690

Gramoli, V. (2016). On the danger of private blockchains. In *Workshop on distributed cryptocurrencies and consensus ledgers (dccl'16).*

Granjal, J., Monteiro, E., & Silva, J. S. (2010, 12). Enabling Network-Layer Security on IPv6 Wireless Sensor Networks. In *2010 ieee global telecommunications conference globecom 2010* (pp. 1–6). IEEE. Retrieved from http://ieeexplore.ieee.org/document/5684293/ doi: 10.1109/GLOCOM.2010.5684293

Gupta, Shorey, R., Kulkarni, D., & Tew, J. (2018, 1). The applicability of blockchain in the Internet of Things. In *2018 10th international conference on communication systems & networks (comsnets)* (pp. 561–564). IEEE. Retrieved from http://ieeexplore.ieee.org/document/8328273/ doi: 10.1109/COMSNETS.2018.8328273

Gupta, Vanbever, L., Shahbaz, M., Donovan, S., Schlinker, B., Feamster, N., ... Katz-Bassett, E. (2014, 2). SDX: A software defined Internet exchange. *ACM SIGCOMM Computer Communication Review*, *44*(4), 579–580. Retrieved from https://dl.acm.org/doi/10.1145/2740070.2626300 doi: 10.1145/2740070.2626300

Hajizadeh, M., Afraz, N., Ruffini, M., & Bauschert, T. (2020). Collaborative cyber attack defense in SDN networks using blockchain technology. In *Proceedings of the 2020 ieee conference on network softwarization: Bridging the gap between ai and network softwarization, netsoft 2020* (pp. 487–492). Retrieved from https://www.researchgate.net/publication/343616521 doi: 10.1109/NetSoft48620.2020.9165396

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018, 9). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142. Retrieved from `https://www-sciencedirect-com.ezproxy.lib.purdue.edu/science/article/pii/S0167404818300890` doi: 10.1016/J.COSE.2018.06.004

He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th usenix security symposium (usenix security 18)* (pp. 255–272). Retrieved from `https://www.usenix.org/conference/usenixsecurity18/presentation/he`

Hoy, M. B. (2017, 7). An Introduction to the Blockchain and Its Implications for Libraries and Medicine. *Medical Reference Services Quarterly*, *36*(3), 273–279. Retrieved from `https://www.tandfonline.com/doi/full/10.1080/02763869.2017.1332261` doi: 10.1080/02763869.2017.1332261

Huang, X., Xiang, Y., Bertino, E., Zhou, J., & Xu, L. (2014, 11). Robust Multi-Factor Authentication for Fragile Communications. *IEEE Transactions on Dependable and Secure Computing*, *11*(6), 568–581. Retrieved from `http://ieeexplore.ieee.org/document/6701152/` doi: 10.1109/TDSC.2013.2297110

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019, 12). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129. doi: 10.1016/j.ijinfomgt.2019.02.005

Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In *2017 19th international conference on advanced communication technology (icact)* (pp. 464–467). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7890132/` doi: 10.23919/ICACT.2017.7890132

Jasper, S. E. (2017, 1). U.S. Cyber Threat Intelligence Sharing Frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53–65. Retrieved from `https://www.tandfonline.com/doi/abs/10.1080/08850607.2016.1230701` doi: 10.1080/08850607.2016.1230701

Jerkins, J. A. (2017, 1). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. In *2017 ieee 7th annual computing and communication workshop and conference (ccwc)* (pp. 1–5). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7868464/` doi: 10.1109/CCWC.2017.7868464

Karamanos, E. (2010). *Investigation of home router security.*

Karame, G., & Ghassan. (2016). On the Security and Scalability of Bitcoin's Blockchain. In *Proceedings of the 2016 acm sigsac conference on computer and communications security - ccs'16* (pp. 1861–1862). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?doid=2976749.2976756 doi: 10.1145/2976749.2976756

Kareem, A., Bin Sulaiman, R., & Umer Farooq, M. (2018, 8). Algorithms and Security Concern in Blockchain Technology: A Brief Review. *SSRN Electronic Journal*. Retrieved from https://www.ssrn.com/abstract=3234933 doi: 10.2139/ssrn.3234933

Khan, M. A., & Salah, K. (2018, 5). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167739X17315765 doi: 10.1016/J.FUTURE.2017.11.022

Kiayias, A., & Panagiotakos, G. (2015). Speed-Security Tradeoffs s in Blockchain Protocols. *Cryptology ePrint Archive*, 6. Retrieved from https://www.semanticscholar.org/paper/Speed-Security-Tradeo-s-in-Blockchain-Protocols-Kiayias/62646f9450a3c95e745c1d2bb056dcf851acdaadhttp://eprint.iacr.org/2015/1019 doi: 10.1109/IOT.2014.7030106

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84.

Kolisnyk, M., & Kharchenko, V. (2019). A Markov Model of IoT System Availability Considering DDoS Attacks, Patching and Energy Modes. In (pp. 185–207). Springer, Cham. Retrieved from http://link.springer.com/10.1007/978-3-030-00253-4_9 doi: 10.1007/978-3-030-00253-4{_}9

Koponen, T., Casado, M., Gude, N., Stribling, J., Poutievski, L., Zhu, M., … Shenker, S. (2019). Onix: A distributed control platform for large-scale production networks. In *Proceedings of the 9th usenix symposium on operating systems design and implementation, osdi 2010* (pp. 351–364).

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013, 11). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, *11*(8), 2710–2723. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1570870513001029 doi: 10.1016/J.ADHOC.2013.05.003

Krebs, B. (2016). *DDoS on Dyn Impacts Twitter, Spotify, Reddit.* Retrieved from https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify

Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional*, *19*(4), 68–72. Retrieved from `http://ieeexplore.ieee.org/document/8012302/` doi: 10.1109/MITP.2017.3051335

Kumar, M., Kumar, S., Budhiraja, R., Das, M., & Singh, S. (2016, 12). Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach. In *2016 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata)* (pp. 424–428). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7917128/` doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100

Lee, B., & Lee, J.-H. (2017, 3). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *The Journal of Supercomputing*, *73*(3), 1152–1167. Retrieved from `http://link.springer.com/10.1007/s11227-016-1870-0` doi: 10.1007/s11227-016-1870-0

Li, Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017, 8). A survey on the security of blockchain systems. *Future Generation Computer Systems*. Retrieved from `https://www.sciencedirect.com/science/article/pii/S0167739X17318332` doi: 10.1016/J.FUTURE.2017.08.020

Li, & Trappe, W. (2006, 10). Light-weight Detection of Spoofing Attacks in Wireless Networks. In *2006 ieee international conference on mobile ad hoc and sensor sysetems* (pp. 845–851). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/4054009/` doi: 10.1109/MOBHOC.2006.278663

Li, V. G., Dunn, M., Pearce, P., McCoy, D., Voelker, G. M., Savage, S., & Levchenko, K. (2019). Reading the tea leaves: A comparative analysis of threat intelligence. In *Proceedings of the 28th usenix security symposium* (pp. 851–867). Retrieved from `https://www.usenix.org/conference/usenixsecurity19/presentation/li`

Liu, Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, 6). Blockchain Based Data Integrity Service Framework for IoT Data. In *2017 ieee international conference on web services (icws)* (pp. 468–475). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/8029796/` doi: 10.1109/ICWS.2017.54

Liu, Zhang, Y., & Zhang, H. (2013, 12). A Novel Approach to IoT Security Based on Immunology. In *2013 ninth international conference on computational intelligence and security* (pp. 771–775). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/6746536/` doi: 10.1109/CIS.2013.168

Lohachab, A., & Karambir, B. (2018, 9). Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. *Journal of Communications and Information Networks*, *3*(3), 57–78. Retrieved from `http://link.springer.com/10.1007/s41650-018-0022-5` doi: 10.1007/s41650-018-0022-5

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. R. (2013). *Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things* (Vol. 1; Tech. Rep. No. 4). Retrieved from `http://vbn.aau.dk/files/74574200/PNM_IACAC_River.pdf`

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, 12). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th international conference for internet technology and secured transactions (icitst)* (pp. 336–341). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7412116/` doi: 10.1109/ICITST.2015.7412116

Manikumar, D. V., & Maheswari, B. U. (2020, 7). Blockchain Based DDoS Mitigation Using Machine Learning Techniques. In *Proceedings of the 2nd international conference on inventive research in computing applications, icirca 2020* (pp. 794–800). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ICIRCA48905.2020.9183092

Mcmahon, D., Canada, B., & Howes, R. (2013). *The Dark Space Project The Dark Space Project* (Tech. Rep. No. July). Defence R & D Canada – Centre for Security Science.

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162–182. Retrieved from `https://www.tandfonline.com/doi/full/10.1080/19393555.2018.1458258` doi: 10.1080/19393555.2018.1458258

Mendez Mena, D., & Yang, B. (2018). Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks. In *Proceedings of the 19th annual sig conference on information technology education* (pp. 7–12). Retrieved from `https://dl.acm.org/citation.cfm?id=3241853https://doi.org/10.1145/3241815.3241853` doi: 10.1145/3241815.3241853

Mendez Mena, D., & Yang, B. (2020). Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things. *IoT*, *2*(1), 1–16. Retrieved from `https://www.mdpi.com/2624-831X/2/1/1` doi: 10.3390/iot2010001

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the internet of things (iot). *IEEE Internet Initiative*, *1*(1), 1–86.

Misra, S., Deb, P. K., Pathak, N., & Mukherjee, A. (2020, 7). Blockchain-enabled SDN for securing fog-based resource-constrained IoT. In *Ieee infocom 2020 - ieee conference on computer communications workshops, infocom wkshps 2020* (pp. 490–495). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/INFOCOMWKSHPS50562.2020.9162706

Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011). A learning automata based solution for preventing distributed denial of service in Internet of things. In *Internet of things (ithings/cpscom), 2011 international conference on and 4th international conference on cyber, physical and social computing* (pp. 114–122).

Modi, S. (2020). *CERIAS : Value of Cyber Threat Intelligence in Modern Security Operations - Purdue University.* Retrieved from https://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/64djdbglbtmib80a3o6cfusgie

Mtsweni, J., & Mutemwa, M. (2019). Technical Guidelines for Evaluating and Selecting Data Sources for Cybersecurity Threat Intelligence. In *Eccws 2019 18th european conference on cyber warfare and security - google books* (pp. 305–313). Retrieved from https://books.google.com/books?hl=en&lr=&id=b8-hDwAAQBAJ&oi=fnd&pg=PA305&dq=counter+threat+intelligence+challenges&ots=KPM3CE0pxn&sig=yv0MorEDI2XH36scFLZRGBN_Jd8#v=onepage&q=counterthreatintelligencechallenges&f=false

Mylrea, M., & Gourisetti, S. N. G. (2017, 9). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 resilience week (rws)* (pp. 18–23). IEEE. Retrieved from http://ieeexplore.ieee.org/document/8088642/ doi: 10.1109/RWEEK.2017.8088642

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from http://www.academia.edu/download/32413652/BitCoin_P2P_electronic_cash_system.pdf

Noubir, G., & Lin, G. (2003, 7). Low-power DoS attacks in data wireless LANs and countermeasures. *ACM SIGMOBILE Mobile Computing and Communications Review*, *7*(3), 29. Retrieved from http://portal.acm.org/citation.cfm?doid=961268.961277 doi: 10.1145/961268.961277

Novo, O. (2018, 4). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184–1195. Retrieved from https://ieeexplore.ieee.org/document/8306880/ doi: 10.1109/JIOT.2018.2812239

OASIS. (n.d.-a). *CybOX Community (Archive) — CybOX Project Documentation.* Retrieved from https://cyboxproject.github.io/community/

OASIS. (n.d.-b). *Introduction to TAXII.* Retrieved from https://oasis-open.github.io/cti-documentation/taxii/intro.html

OASIS. (2017). *Introduction to STIX.* Retrieved from https://oasis-open.github.io/cti-documentation/stix/intro

Ølnes, S., Ubacht, J., & Janssen, M. (2017, 9). *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing* (Vol. 34) (No. 3). Elsevier Ltd. doi: 10.1016/j.giq.2017.09.007

Oracevic, A., Dilek, S., & Ozdemir, S. (2017, 5). Security in internet of things: A survey. In *2017 international symposium on networks, computers and communications (isncc)* (pp. 1–6). IEEE. Retrieved from http://ieeexplore.ieee.org/document/8072001/ doi: 10.1109/ISNCC.2017.8072001

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016, 12). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks*, *9*(18), 5943–5964. Retrieved from http://doi.wiley.com/10.1002/sec.1748 doi: 10.1002/sec.1748

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In *Advances in intelligent systems and computing* (Vol. 520, pp. 523–533). Springer, Cham. Retrieved from http://link.springer.com/10.1007/978-3-319-46568-5_53 doi: 10.1007/978-3-319-46568-5{_}53

Ourad, A. Z., Belgacem, B., & Salah, K. (2018, 6). Using Blockchain for IOT Access Control and Authentication Management. In *International conference on internet of things* (pp. 150–164). Springer, Cham. Retrieved from http://link.springer.com/10.1007/978-3-319-94370-1_11 doi: 10.1007/978-3-319-94370-1{_}11

OWASP. (2014). *Top IoT Vulnerabilities.* Retrieved from https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

Pacheco, J., & Hariri, S. (2016, 9). IoT Security Framework for Smart Cyber Infrastructures. In *2016 ieee 1st international workshops on foundations and applications of self* systems (fas*w)* (pp. 242–247). IEEE. Retrieved from http://ieeexplore.ieee.org/document/7789475/ doi: 10.1109/FAS-W.2016.58

Park, & Kang, N. (2015, 12). Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle. *Sensors*, *16*(1), 20. Retrieved from http://www.mdpi.com/1424-8220/16/1/20 doi: 10.3390/s16010020

Park, & Park, J. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry*, *9*(8), 164. Retrieved from https://www.mdpi.com/2073-8994/9/8/164http://www.mdpi.com/2073-8994/9/8/164 doi: 10.3390/sym9080164

Peretti, G., Lakkundi, V., & Zorzi, M. (2015, 1). BlinkToSCoAP: An end-to-end security framework for the Internet of Things. In *2015 7th international conference on communication systems and networks (comsnets)* (pp. 1–6). IEEE. Retrieved from http://ieeexplore.ieee.org/document/7098708/ doi: 10.1109/COMSNETS.2015.7098708

Purohit, S., Calyam, P., Wang, S., Yempalla, R. K., & Varghese, J. (2020). DefenseChain, Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense. In *2020 2nd conference on blockchain research and applications for innovative networks and services, brains 2020* (pp. 112–119). Retrieved from https://ieeexplore.ieee.org/abstract/document/9223313/ doi: 10.1109/BRAINS49436.2020.9223313

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018, 3). The Blockchain as a Decentralized Security Framework [Future Directions]. *IEEE Consumer Electronics Magazine*, *7*(2), 18–21. Retrieved from http://ieeexplore.ieee.org/document/8287055/ doi: 10.1109/MCE.2017.2776459

Rajagopalan, A., Jagga, M., Kumari, A., & Ali, S. T. (2017, 2). A DDoS prevention scheme for session resumption SEA architecture in healthcare IoT. In *2017 3rd international conference on computational intelligence & communication technology (cict)* (pp. 1–5). IEEE. Retrieved from http://ieeexplore.ieee.org/document/7977361/ doi: 10.1109/CIACT.2017.7977361

Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics (Switzerland)*, *9*(5). Retrieved from www.mdpi.com/journal/electronics doi: 10.3390/electronics9050824

Raval, S. (2016). *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (First Edit ed.). O'Reilly.

Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2014, 12). Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN. *Security and Communication Networks*, *7*(12), 2654–2668. Retrieved from http://doi.wiley.com/10.1002/sec.406 doi: 10.1002/sec.406

Riaz, R., Kim, K.-H., & Ahmed, H. F. (2009, 3). Security analysis survey and framework design for IP connected LoWPANs. In *2009 international symposium on autonomous decentralized systems* (pp. 1–6). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/5207373/` doi: 10.1109/ISADS.2009.5207373

Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., & Stiller, B. (2017). A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 10356 LNCS, pp. 16–29). Retrieved from `https://www.zora.uzh.ch/id/eprint/146085/` doi: 10.1007/978-3-319-60774-0{_}2

Rodrigues, B., Bocek, T., & Stiller, B. (2016). Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS). *Semantic Scholar*. Retrieved from `https://www.ieeelcn.org/lcn42demos/1570382330.pdf`

Rodrigues, B., Bocek, T., & Stiller, B. (2017, 7). Multi-domain DDoS mitigation based on blockchains. In *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 10356 LNCS, pp. 185–190). Springer Verlag. Retrieved from `https://link.springer.com/chapter/10.1007/978-3-319-60774-0_19` doi: 10.1007/978-3-319-60774-0{_}19

Rodrigues, B., Scheid, E., Killer, C., Franco, M., & Stiller, B. (2020, 10). Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks. *Journal of Network and Systems Management*, *28*(4), 953–989. Retrieved from `https://doi.org/10.1007/s10922-020-09559-4` doi: 10.1007/s10922-020-09559-4

Roman, R., Lopez, J., & Mambo, M. (2018, 1). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680–698. Retrieved from `https://www-sciencedirect-com.ezproxy.lib.purdue.edu/science/article/pii/S0167739X16305635` doi: 10.1016/J.FUTURE.2016.11.009

Sadique, F., Cheung, S., Vakilinia, I., Badsha, S., & Sengupta, S. (2018, 11). Automated Structured Threat Information Expression (STIX) Document Generation with Privacy Preservation. In *2018 9th ieee annual ubiquitous computing, electronics and mobile communication conference, uemcon 2018* (pp. 847–853). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/UEMCON.2018.8796822

Samaila, M. G., Sequeiros, J. B. F., & Correia, A. F. P. P. (2018). A Quick Perspective on the Current State of IoT Security: A Survey. In *Networks of the future* (First Edit ed., pp.

431–464). New York: Chapman and Hall/CRC. Retrieved from https://www.taylorfrancis.com/books/e/9781498783989/chapters/10.1201%2F9781315155517-21

Seitz, L., Selander, G., Wahlstroem, E., & Erdtman, S. (2017). *Authentication and authorization for constrained environments (ace)* (Tech. Rep.). IETF. Retrieved from https://www.ietf.org/proceedings/98/slides/slides-98-ace-authorization-using-oauth-20-00.pdf

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards Blockchain-based Auditable Storage and Sharing of IoT Data. In *Proceedings of the 2017 on cloud computing security workshop - ccsw '17* (pp. 45–50). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?doid=3140649.3140656 doi: 10.1145/3140649.3140656

Sharma, P. K., Singh, S., Jeong, Y.-S., & Park, J. H. (2017). DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. *IEEE Communications Magazine*, *55*(9), 78–85. Retrieved from http://ieeexplore.ieee.org/document/8030491/ doi: 10.1109/MCOM.2017.1700041

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

Siddharth, M. (2020). *DDoS Botnet Attack on IOT Devices — Kaggle.* Retrieved from https://www.kaggle.com/siddharthm1698/ddos-botnet-attack-on-iot-devices

Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016). Smart-Phones Attacking Smart-Homes. In *Proceedings of the 9th acm conference on security & privacy in wireless and mobile networks - wisec '16* (pp. 195–200). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?doid=2939918.2939925 doi: 10.1145/2939918.2939925

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. In *Wireless and mobile computing, networking and communications (wimob), 2015 ieee 11th international conference on* (pp. 163–167).

Strielkina, A., Kharchenko, V., & Uzun, D. (2018, 5). Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities. In *2018 ieee 9th international conference on dependable systems, services and technologies (dessert)* (pp. 58–62). IEEE. Retrieved from https://ieeexplore.ieee.org/document/8409099/ doi: 10.1109/DESSERT.2018.8409099

Sullivan, C., & Burger, E. (2017, 2). “In the public interest”: The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law and Security Review*, *33*(1), 14–29. doi: 10.1016/j.clsr.2016.11.015

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. doi: 10.1109/CANDAR.2017.50

Tapscott, D. (2018). *Blockchain Revolution the Internet of Value*. Retrieved from `https://books.google.com/books?hl=en&lr=&id=NqBiCgAAQBAJ&oi=fnd&pg=PT11&dq=blockchain+&ots=sRxIDLZ6tv&sig=_blElVx2Pi6x8OcPe-jc0u9GFD4`

Tounsi, W., & Rais, H. (2018, 1). *A survey on technical threat intelligence in the age of sophisticated cyber attacks* (Vol. 72). Elsevier Ltd. doi: 10.1016/j.cose.2017.09.001

Tragos, E. Z., Bernabe, J., Staudemeyer, R. C., Luis, J., Ramos, H., Fragkiadakis, A., … Gluhak, A. (2016). Trusted IoT in the complex landscape of governance, security, privacy, availability and safety. In *Digitising the industry-internet of things connecting the physical, digital and virtual worlds* (River Publ ed., pp. 210–239). River Publishers. Retrieved from `http://rcsme.de/dissemination/papers/Tragos_2016_trusted_IoT_preprint.pdf`

Tschofenig, H., Arkko, J., Thaler, D., & McPherson, D. (2015). *Architectural considerations in smart object networking, RFC 7452 (Informational)* (Tech. Rep.). Internet Engineering Task Force. Retrieved from `http://www.rfc-editor.org/info/rfc7452`

Underwood, S., & Sarah. (2016, 10). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. Retrieved from `http://dl.acm.org/citation.cfm?doid=3013530.2994581` doi: 10.1145/2994581

Verizon. (2015). *Verizon 2015 Data Breach Investigations Report Finds Cyberthreats Are Increasing in Sophistication — About Verizon.* Retrieved from `https://www.verizon.com/about/news/2015-verizon-dbir-report-security`

Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015, 9). OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Networks*, *32*, 3–16. Retrieved from `https://www.sciencedirect.com/science/article/abs/pii/S1570870514003126` doi: 10.1016/J.ADHOC.2014.12.005

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016, 10). MISP - The design and implementation of a collaborative threat intelligence sharing platform. In *Wiscs 2016 - proceedings of the 2016 acm workshop on information sharing and collaborative security, co-located with ccs 2016* (pp. 49–56). New York, New York, USA: Association for Computing Machinery, Inc. Retrieved from `http://dl.acm.org/citation.cfm?doid=2994539.2994542` doi: 10.1145/2994539.2994542

Wang, Z., Dong, X., Li, Y., Fang, L., & Chen, P. (2018, 8). IoT Security Model and Performance Evaluation: A Blockchain Approach. In *2018 international conference on network infrastructure and digital content (ic-nidc)* (pp. 260–264). IEEE. Retrieved from `https://ieeexplore.ieee.org/document/8525716/` doi: 10.1109/ICNIDC.2018.8525716

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021, 1). Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry*, *13*(2), 227. Retrieved from `https://www.mdpi.com/2073-8994/13/2/227` doi: 10.3390/sym13020227

Web Of Science. (n.d.). *Web of Science [v.5.31] - Web of Science Core Collection Result Analysis.* Retrieved from `https://wcs-webofknowledge-com.ezproxy.lib.purdue.edu/RA/analyze.do?product=WOS&SID=7BznYoQC7nXztoyS6z7&field=PY_PublicationYear_PublicationYear_en&yearSort=true`

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30.

Wessling, F., Ehmke, C., Hesenius, M., & Gruhn, V. (2018). How Much Blockchain Do You Need? Towards a Concept for Building Hybrid DApp Architectures. In *2018 ieee/acm 1st international workshop on emerging trends in software engineering for blockchain (wetseb)* (pp. 44–47). Retrieved from `https://ieeexplore.ieee.org/abstract/document/8445058/` doi: 10.1145/3194113.3194121

Wiederhold, B. K., Riva, G., & Graffigna, G. (2014). *A next-generation smart contract and decentralized application platform.* Ethereum White Paper. Retrieved from `https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf` doi: 10.5663/aps.v1i1.10138

Wu, Y., Qiao, Y., Ye, Y., & Lee, B. (2019). Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In *2019 6th international conference on internet of things: Systems, management and security, iotsms 2019* (pp. 474–481). Retrieved from `https://doi.org/10.1109/IOTSMS48152.2019.8939192` doi: 10.1109/IOTSMS48152.2019.8939192

Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., & Jin, Y. (2016, 1). Security analysis on consumer and industrial IoT devices. In *2016 21st asia and south pacific design automation conference (asp-dac)* (pp. 519–524). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/7428064/` doi: 10.1109/ASPDAC.2016.7428064

Xiao, L., Greenstein, L., Mandayam, N., & Trappe, W. (2007, 6). Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication. In *2007 ieee international conference on communications* (pp. 4646–4651). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/4289438/` doi: 10.1109/ICC.2007.767

Xie, Y., & Wang, D. (2014, 4). An Item-Level Access Control Framework for Inter-System Security in the Internet of Things. *Applied Mechanics and Materials*, *548-549*, 1430–1432. Retrieved from `https://www.scientific.net/AMM.548-549.1430` doi: 10.4028/www.scientific.net/AMM.548-549.1430

Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th acm international symposium on mobile ad hoc networking and computing - mobihoc '05* (p. 46). New York, New York, USA: ACM Press. Retrieved from `http://portal.acm.org/citation.cfm?doid=1062689.1062697` doi: 10.1145/1062689.1062697

Xu, W., Wood, T., Trappe, W., & Zhang, Y. (2004). Channel surfing and spatial retreats. In *Proceedings of the 2004 acm workshop on wireless security - wise '04* (p. 80). New York, New York, USA: ACM Press. Retrieved from `http://portal.acm.org/citation.cfm?doid=1023646.1023661` doi: 10.1145/1023646.1023661

Yan, Z., Kantola, R., & Shen, Y. (2011, 11). Unwanted traffic control via global trust management. In *Proc. 10th ieee int. conf. on trust, security and privacy in computing and communications, trustcom 2011, 8th ieee int. conf. on embedded software and systems, icess 2011, 6th int. conf. on fcst 2011* (pp. 647–654). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/6120876/` doi: 10.1109/TrustCom.2011.83

Yeh, K.-H. (2016). BSNCare+: A Robust IoT-Oriented Healthcare System with Non-Repudiation Transactions. *Applied Sciences*, *6*(12), 418.

Yiakoumis, Y., Yap, K.-K., Katti, S., Parulkar, G., & McKeown, N. (2011). Slicing home networks. In *Proceedings of the 2nd acm sigcomm workshop on home networks* (pp. 1–6).

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016, 10). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE*, *11*(10), e0163477. Retrieved from `https://dx.plos.org/10.1371/journal.pone.0163477` doi: 10.1371/journal.pone.0163477

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices. In *Proceedings of the 14th acm workshop on hot topics in networks -*

hotnets-xiv (pp. 1–7). New York, New York, USA: ACM Press. Retrieved from `http://dl.acm.org/citation.cfm?doid=2834050.2834095` doi: 10.1145/2834050.2834095

Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014, 11). IoT Security: Ongoing Challenges and Research Opportunities. In *2014 ieee 7th international conference on service-oriented computing and applications* (pp. 230–234). IEEE. Retrieved from `http://ieeexplore.ieee.org/document/6978614/` doi: 10.1109/SOCA.2014.58

Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *Int. J. Web and Grid Services*, *14*(4), 352–375. Retrieved from `https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf` doi: 10.1504/IJWGS.2018.095647

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017, 1). Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26–33. Retrieved from `http://ieeexplore.ieee.org/document/7823334/` doi: 10.1109/MCOM.2017.1600363CM

Zyskind, G., Nathan, O., & others. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Security and privacy workshops (spw), 2015 ieee* (pp. 180–184).

VITA

VITA

- **Education**
  - Ph.D. Technology, Purdue University May 2021
    West Lafayette, IN

    Specialization: Information Security

    Principal Advisor: Baijian Yang, Ph.D.

    Dissertation: Blockchain-Based Security Framework for the Internet of Things and Home Networks.
  - M.S. Computer and Information Technology, Purdue University, May 2013
    West Lafayette, IN
  - B.S. Electronic Engineering, Army Polytechnic School, Ecuador October 2009
- **Fields of Interest**

  Cyber Security, Blockchain, Internet of Things Security, Network Security, Incident Response, STEM Fostering.
- **Professional Memberships**
  - Association for Computing Machinery 2018 - 2019
  - Society of Hispanic Professional Engineers 2017-2018
- **Publications**
  - Mendez Mena, D. & Yang, B. (2018). Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things *IoT*, 2(1), 1-16.
  - Mendez Mena, D. & Yang, B. (2018). Blockchain-Based Whitelisting for Consumer IoT Devices and Home Networks *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, 2018, 7-12.
  - Mendez Mena, D., Papapanagiotou I. & Yang, B. (2018). Internet of Things: Survey on Security *Information Security Journal: A Global Perspective*, 27(3), 162-182.

  - Mendez Mena, D. & Serrano, M. (2013, March). Using Twitter to Engage Ecuadorian High School Students in STEM. In *Society for Information Technology & Teacher Education International Conference* (Vol. 2013, No. 1, pp. 3522-3529).

- **Awards**
  - Purdue University 5 Students Who are Transformation Makers 2012-2013
- **Professional Certifications**
  - GIAC Incident Handler Certification 2016-Present
  - Cisco Certified Network Professional Routing & Switching 2010-2020
  - Cisco Certified Design Professional 2010-2020
  - Cisco Certified Network Associate Security 2010-2020
- **Professional Experience**
  - IT Security Lead Analyst, Zimmer Biomet, Warsaw, IN 2013-Present
    Responsibilities: Incident Response, Network Perimeter Security, Security Information and Event Management.
  - IT Network Intern, Zimmer Biomet, Warsaw, IN, June - August 2012
    Responsibilities: Simple Management Network Protocol Enhancement Project, Bandwidth Efficiency Analysis.
  - Pre-sales Post Sales Engineering Supervisor, Totaltek, Quito - Ecuador, 2008 - 2010
    Responsibilities: Network Design and Implementation, Routing, Switching, Voice over IP, Perimeter Security, Bandwidth Management.